Milnorin lause

Äärellisesti viritettyjen ratkeavien ryhmien kasvusta

Helsingin yliopisto

Matematiikan ja tilastotieteen osasto

Pro gradu -tutkielma

Lilja Metsälampi

Ohjaaja:

Prof. Pekka Pankka

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen osasto

Tekijä — Författare — Author

Lilja Metsälampi

Työn nimi — Arbetets titel — Title

Milnorin lause äärellisesti viritettyjen ratkeavien ryhmien kasvusta

Oppiaine — Läroämne — Subject

Matematiikka

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Lokakuu 2021	61 s.

Tiivistelmä — Referat — Abstract

Tutkielman päämääränä on esitellä ja todistaa Milnorin lause (John Milnor, 1968) geometrisen ryhmäteorian alalta. Milnorin lause on olennainen osa äärellisesti viritettyjen ratkeavien ryhmien kasvun luokittelua. Se kertoo, että äärellisesti viritetyt ratkeavat ryhmät joko kasvavat eksponentiaalisesti tai ovat polysyklisiä. Polysyklisten ryhmien kasvun tiedetään olevan joko polynomista tai eksponentiaalista. Näin ollen äärellisesti viritetyt ratkeavat ryhmät kasvavat joko polynomisesti tai eksponentiaalisesti.

Tutkielman ensimmäinen luku on johdantoa ja toinen luku on esitietoja. Tutkielman kolmannessa luvussa esitellään ryhmät ja aakkostot. Erityisesti esitellään, mitä tarkoittaa ajatella ryhmän alkioita jonkin aakkoston sanoina. Lisäksi määritellään vapaat ryhmät ja ryhmien esitykset. Tämän jälkeen neljännessä luvussa ryhmiin määritellään ryhmän Cayley graafin avulla sanametriikaksi kutsuttu metriikka. Todistetaan, että eri virittäjäjoukkojen suhteen muodostetut sanametriikat ovat keskenään bilipschitzekvivalentit. Lopulta määritellään ryhmien kasvu ja todistetaan, että ryhmän kasvu ei riipu valitusta virittäjäjoukosta.

Viidennessä luvussa esitellään ratkeavat ryhmät, nilpotentit ryhmät ja polysykliset ryhmät ja muutamia konkreettisia esimerkkejä näistä ryhmistä. Lisäksi esitellään näiden ryhmien keskeisiä ominaisuuksia ja niiden välisiä suhteita. Todistetaan esimerkiksi, että jokainen nilpotentti ja polysyklinen ryhmä on myös ratkeava ryhmä.

Kuudennessa luvussa todistetaan tutkielman päätulos, Milnorin lause. Se tapahtuu induktiolla ratkeavalle ryhmälle ominaisen subnormaalin laskevan jonon pituuden suhteen. Lisäksi esitellään ja todistetaan tarvittavia aputuloksia. Luvun lopussa esitellään Wolfin lause (Joseph Wolf, 1968) ja yhdistetään Milnorin ja Wolfin lauseet yhdeksi tulokseksi, Milnor-Wolfin lauseeksi. Milnor-Wolfin lauseen nojalla äärellisesti viritettyjen ratkeavien ryhmien kasvu saadaan luokiteltua.

Avainsanat — Nyckelord — Keywords

Geometrinen ryhmäteoria, Ratkeavat ryhmät, Polysykliset ryhmät, Ryhmien kasvu

Säilytyspaikka — Förvaringsställe — Where deposited

Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Sisällys

Luku 1

Johdanto

Tämä tutkielma käsittelee John Milnorin lausetta geometrisen ryhmäteorian alalta. Geometrinen ryhmäteoria on matematiikan ala, jossa perusideana on käsitellä ryhmiä geometrisina tai topologisina avaruuksina.

Tässä tutkielmassa tarkastellaan äärellisesti viritettyjä ryhmiä. Äärellisesti viritettyyn ryhmään G, jonka virittäjäjoukko on S, voidaan yhdistää yhtenäinen graafi, jota kutsutaan ryhmän G *Cayley graafiksi*. Tämän graafin avulla ryhmään G voidaan määritellä *sanametriikaksi* kutsuttu metriikka. Ryhmän alkioiden väliseksi etäisyydeksi määritellään niitä vastaavien solmujen etäisyys Cayley graafissa.

Kun ryhmään on määritelty metriikka, voidaan tutkia *ryhmän kasvua*. Metrisessä avaruudessa (G, dist_S) suljetun r-säteisen kuulan mahtavuutta kutsutaan *kasvufunktioksi*. Virittäjäjoukon valinta vaikuttaa itse kasvufunktioon, mutta ryhmän *kasvun nopeuteen* tai *tahtiin* ei. Tämä seuraa siitä, että kasvun nopeus on kvasi-isometria invariantti. Näin ollen voidaan puhua *ryhmän kasvusta*, mikä voi olla esimerkiksi polynomista tai eksponentiaalista.

Tässä tutkielmassa tarkastellaan äärellisesti viritettyjä ratkeavia ryhmiä ja niiden kasvua. Päämääränä on todistaa Milnorin lause [8]:

Lause 1.1. Jokainen äärellisesti viritetty ratkeava ryhmä joko kasvaa eksponentiaalisesti tai on polysyklinen.

Yhdistettynä Wolfin lauseeseen [12], jonka mukaan jokainen polysyklinen ryhmä on joko *melkein* nilpotentti tai se kasvaa eksponentiaalisesti, äärellisesti viritettyjen ratkeavien ryhmien kasvu saadaan luokiteltua.

Jokainen äärellisesti viritetty nilpotentti ryhmä on polysyklinen, mutta on olemassa polysyklisiä ryhmiä, jotka eivät ole nilpotentteja. Lisäksi jokainen polysyklinen ryhmä on ratkeava, mutta on olemassa äärellisesti viritettyjä ratkeavia ryhmiä, jotka eivät ole polysyklisiä. Eräs esimerkki tällaisesta ryhmästä on *Baumslag-Solitar ryhmä* $BS(1,2) = \langle a, b \mid aba^{-1} = b^2 \rangle$ [2, section 13.8]. Näin ollen myös jokainen äärellisesti viritetty nilptentti ryhmä on ratkeava

Nilpotenteilla ryhmillä on todistettu olevan polynominen kasvu, joten yhdistämällä Milnorin ja Wolfin tulokset yhteen lauseeseen saadaan tulos, joka kertoo, että äärellisesti viritetyt ratkeavat ryhmät kasvavat joko polynomisesti tai eksponentiaalisesti. Tämä tulos ei päde yleisesti äärellisesti viritetyille ryhmille: on olemassa äärellisesti viritettyjä ryhmiä, joiden kasvun nopeus on polynomisen ja eksponentiaalisen kasvun väliltä [3]. Toisaalta jokainen äärellisesti viritetty ryhmä, joka kasvaa polynomisesti, on *melkein* nilpotentti [4].

Tämä tutkielma on jäsennelty seuraavasti. Esitietojen jälkeen pohjustetaan ryhmät ja aakkostot. Esitellään, mitä tarkoittaa ajatella ryhmän alkioita jonkin aakkoston *sanoina*, vapaat ryhmät ja ryhmien esitykset, jotka ovat tarpeellisia monissa tämän tutkielman todituksissa. Näiden jälkeen määritellään ryhmiin metriikka ja ryhmien kasvu. Ryhmien kasvuun liittyvien tulosten jälkeen siirrytään tutkielman algebralliseen osuuteen. Lukuun 5 on koottu ratkeavien, polysyklisten ja nilpotenttien ryhmien määritelmät sekä näiden ominaisuuksia. Viimeisessä luvussa todistetaan Milnorin lause ja Milnorin lauseen todistuksessa käytettävät aputulokset. Aivan lopuksi liitetään Milnorin ja Wolfin lauseet yhdeksi tulokseksi, jonka avulla äärellisesti viritettyjen ratkeavien ryhmien kasvu saadaan luokiteltua.

Päälähteenä tässä tutkielmassa on käytetty kirjaa [2], josta löytyy lisää tietoa geometrisesta ryhmäteoriasta ja aiheista, joita vain sivutaan tässä tutkielmassa kuten esimerkiksi nilpotenttien ryhmien kasvusta. Algebrallisissa osioissa on käytetty apuna myös erityisesti kirjoja [9] ja [10]. Graafeja käsittelevässä kappaleessa on käytetty kirjaa [11]. Kuitenkin myös muita kirjoja on käytetty lähteinä teoriaa ja esimerkkejä varten. Nämä kirjat ovat lueteltuna Kirjallisuutta-osiossa.

Luku 2

Esitietoja

2.1 Ryhmien teoriaan liittyviä tuloksia ja käsitteitä

Tämän aliluvun aiheena on erityisesti tässä työssä tarvittavat ryhmien perustulokset. Lukijan oletetaan tuntevan ryhmän ja aliryhmän määritelmät sekä normaalit aliryhmät, joiden avulla muodostetaan tekijäryhmiä. Lisäksi ryhmien homomorfialause (ks. [7, lause 21.1]), jota usein englanniksi kutsutaan ensimmäiseksi isomorfialauseeksi, oletetaan tunnetuksi.

Esitellään tekijäryhmiin ja normaaleihin aliryhmiin liittyvät 1. isomorfialause ja 2. isomorfialause. Kaikkiin tuloksiin ei liitetä todistusta mukaan, mutta ne löytyvät monista ryhmien teoriaa käsittelevistä teoksista. Tässä alaluvussa on käytetty lähteinä erityisesti kirjoja [9] ja [10].

Lisäksi esitellään ryhmien subnormaalit jonot ja ryhmät, joilla on jokin ominaisuus *melkein*. Näitä tuloksia tarvitaan kappaleessa 3, kun esitetään erilaisia nilpotentteihin, ratkeaviin ja polysyklisiin ryhmiin liittyviä tuloksia. Nämä tulokset ovat kirjasta [2].

Esitellään ensimmäiseksi kolme tulosta, joiden avulla voidaan selvittää, millon kahden ryhmän aliryhmän tulo on myös aliryhmä. Nämä tulokset tulevat tarpeeseen monissa todistuksissa, joissa esiintyy subnormaaleja jonoja.

Lause 2.1. Oletetaan, että G on ryhmä ja että H ja K ovat sen aliryhmiä. Tällöin HK on ryhmän G aliryhmä, jos ja vain jos $HK = KH$.

Todistus. Oletetaan ensin, että HK on ryhmän G aliryhmä, ja olkoon $x \in HK$. Tällöin $x^{-1} \in HK$, sillä HK on aliryhmä. Alkio x^{-1} voidaan kirjoittaa muodossa

hk jollain $h \in H$ ja $k \in K$. Nyt $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$. Siispä $HK \subset KH$. Jos $y \in KH$, niin on olemassa $k \in K$ ja $h \in H$, joilla $y = kh$. Tällöin $y = kh = (h^{-1}k^{-1})^{-1}$, missä $h^{-1}k^{-1} \in HK$. Tällöin myös $(h^{-1}k^{-1})^{-1} \in HK$, sillä oletusten nojalla HK on ryhmän G aliryhmä. Näin ollen $y \in HK$, joten $KH \subset HK$. Näin ollen $HK = KH$.

Oletetaan sitten, että $HK = KH$. Osoitetaan aliryhmäkriteerillä, että HK on ryhmän G aliryhmä. Koska H ja K ovat ryhmän G aliryhmiä, niin erityisesti $1_G \in H$ ja $1_G \in K$. Tällöin $1_G \in HK$ eli erityisesti $HK \neq \emptyset$. Olkoon $x, y \in HK$. Tällöin $x = h_1k_1$ ja $y = h_2k_2$ joillain $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. Halutaan osoittaa, että $xy^{-1} = h_1k_1(h_2k_2)^{-1} \in HK$. Suoraan laskemalla saadaan, että

$$xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1(k_1k_2^{-1}h_2^{-1}),$$

missä $k_1k_2^{-1}h_2^{-1} \in KH = HK$. Näin ollen $k_1k_2^{-1}h_2^{-1}$ on muotoa hk, joillain $h \in H$ ja $k \in K$. Koska H on aliryhmä, niin $h_1h \in H$. Näin ollen

$$xy^{-1} = h_1k_1(h_2k_2)^{-1} = h_1hk \in HK,$$

joten aliryhmäkriteerin nojalla HK on ryhmän G aliryhmä. □

Lause 2.2. Oletetaan, että G on ryhmä ja H ja K ovat sen aliryhmiä. Jos lisäksi K on normaali, niin HK on ryhmän G aliryhmä.

Todistus. Osoitetaan, että HK on aliryhmä. Koska $1_G \in H$ ja $1_G \in K$, niin $1_G \in HK$. Oletetaan sitten, että $h_1, h_2 \in H$ ja $k_1, k_2 \in K$. Nyt voidaan tarkastella alkioiden h_1k_1, h_2k_2 tuloa

$$h_1k_1 \cdot h_2k_2 = h_1h_2(h_2)^{-1}k_1h_2k_2 = h_1h_2kk_2 \in HK,$$

missä $k = (h_2)^{-1}k_1h_2 \in K$, sillä K on normaali. Joukko HK on siis suljettu ryhmän G laskutoimituksen suhteen.

Vastaavasti aliryhmän K normaaliudesta seuraa, että

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h_1^{-1}h_1k_1^{-1}h_1^{-1} = h_1^{-1}k \in HK,$$

missä $k = h_1k_1^{-1}h_1^{-1} \in K$.

Näin ollen HK on ryhmän G aliryhmä. □

Lause 2.3. Olkoon G ryhmä ja H ja N normaaleja aliryhmiä. Tällöin myös HN on normaali.

Todistus. Lauseen 2.2 nojalla HN on ryhmän G aliryhmä. Oletetaan, että $g \in G$ ja $hn \in HN$. Tällöin $ghg^{-1} \in H$ ja $gng^{-1} \in N$. Näin ollen

$$ghng^{-1} = ghg^{-1}gng^{-1} \in HN,$$

joten normaaliuskriteerin nojalla HN on normaali. □

Määritelmä 2.4 (Homomorfismin hajottaminen kulkemaan tekijäryhmän kautta)**.** Olkoon G ja H ryhmiä. Olkoon lisäksi N normaali aliryhmä ja $f\colon G \to H$ homomorfismi. Merkitään tekijähomomorfismia $p\colon G \to G/N$.

Sanotaan, että homomorfismi f voidaan *hajottaa kulkemaan* tekijäryhmän G/N kautta, jos on olemassa sellainen yksikäsitteinen homomorfismi $\bar{f}\colon G/N \to H$, että $f = \bar{f} \circ p$.

Homomorfismin f hajottamisen ideaa voidaan havainnollistaa kaaviolla. Homomorfismi $\bar{f}$ on siis sellainen, että alla oleva kaavio kommutoi

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "p"'] & H \\ G/N \arrow[ur, "\bar{f}"] & \end{tikzcd}$$

Englanniksi kuvauksen hajottamiselle käytetään käsitettä *factor through*, joka käännetään suomeksi usein kuvauksen *faktoroimiseksi*.

Lemma 2.5. Olkoon $f : G \to H$ ryhmähomomorfismi ja N ryhmän G normaali aliryhmä. Homomorfismi f voidaan hajottaa kulkemaan tekijäryhmän G/N kautta, jos $N \subset \ker f$.

Todistus. Oletetaan, että $N \subset \ker f$. Määritellään kuvaus $\bar{f} : G/N \to H$ luonnollisella tavalla säännöllä $gN \mapsto f(g)$. Jos $gN, hN \in G/N$ sellaisia alkioita, joille pätee $gN = hN$, niin $h^{-1}g \in N$. Oletusten nojalla $f(h^{-1}g) = 1_H$, mistä seuraa $f(g) = f(h)$. Näin ollen $\bar{f}(gN) = \bar{f}(hN)$, eli $\bar{f}$ on hyvin määritelty. Kuvaus $\bar{f}$ on homomorfismi, sillä $\bar{f}(gNhN) = \bar{f}(ghN) = f(gh) = f(g)f(h) = \bar{f}(gN)\bar{f}(hN)$ kaikilla $gN, hN \in G/N$. Lisäksi jokaisella $g \in G$ pätee $\bar{f} \circ p(g) = \bar{f}(gN) = f(g)$.

Osoitetaan sitten, että $\bar{f}$ on yksikäsitteinen. Oletetaan, että φ on toinen homomorfismi, jolle pätee $\varphi \circ p = f$. Tällöin jokaisella $g \in G$ pätee $\varphi(gN) = f(g) = \bar{f}(gN)$, eli $\varphi = \bar{f}$. Näin ollen, jos $N \subset \ker f$, niin f voidaan hajottaa kulkemaan tekijäryhmän G/N kautta. □

Lemma 2.5 on ryhmien teorian tulos, joka vastaa yleisempää tilannetta kuin ryhmien homomorfialause. Olettamalla, että $N = \ker f$, lemmasta 2.5 saadaan erikoistapauksena johdettua ryhmien homomorfialause.

Seuraavaksi esiteltävät ryhmien isomorfialauseet löytyvät todistuksineen useimmista ryhmien teoriaa käsittelevistä teoksista. Lause 2.8 on kirjasta [2]. Nämä tulokset antavat hyödyllisiä isomorfismejä eri tekijäryhmien välille, ja niitä käytetään monissa todituksissa, joissa on subnormaaleja jonoja (ks. määritelmä 2.9).

Tässä tutkielmassa käytetään seuraavia merkintöjä ilmaisemaan aliryhmiä ja normaaleja aliryhmiä. Merkinnöillä $H \leqslant G$ ja $H < G$ tarkoitetaan, että H on ryhmän G aliryhmä. Merkinnöillä $N \triangleleft G$ ja $N \trianglelefteq G$ puolestaan tarkoitetaan, että N on ryhmän G normaali aliryhmä.

Lause 2.6 (1. isomorfialause)**.** Olkoot G ryhmä ja H ja N sen aliryhmiä. Oletetaan, että N on lisäksi normaali ryhmässä G. Tällöin $N \triangleleft HN$, $H \cap N \triangleleft H$ ja

$$HN/N \cong H/(H \cap N).$$

Lause 2.7 (2. isomorfialause)**.** Olkoot H ja K ryhmän G normaaleja aliryhmiä, joille pätee $K \leqslant H$. Tällöin tekijäryhmä H/K on normaali ryhmässä G/K, ja

$$(G/K)/(H/K) \cong G/H.$$

Lause 2.8. Jos G on ryhmä, $N \triangleleft G$ ja $A \triangleleft B < G$, niin

$$BN/AN \cong B/A(B \cap N).$$

Määritelmä 2.9 (Subnormaali laskeva jono)**.** Olkoon G ryhmä. Jonoa

$$G = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_n \triangleright \cdots ,$$

missä N_{i+1} on ryhmän N_i normaali aliryhmä kaikilla $i \geq 0$, kutsutaan *subnormaaliksi laskevaksi jonoksi.* Jos lisäksi jokainen ryhmä N_i on normaali ryhmässä G, niin jonoa kutsutaan *normaaliksi jonoksi.* Tekijäryhmiä N_i/N_{i+1} kutsutaan *jonon tekijöiksi.*

Määritelmä 2.10. Oletetaan, että ryhmällä G on subnormaalit laskevat jonot

$$G = A_0 \triangleright A_1 \triangleright \cdots \triangleright A_n = \{1\} \quad \text{ja} \quad G = B_0 \triangleright B_1 \triangleright \cdots \triangleright B_m = \{1\}.$$

Jonoja kutsutaan *isomorfisiksi*, jos

1. $n = m$ ja
2. on olemassa sellainen bijektio

$$f\colon \{A_i/A_{i+1} \mid i = 0, \dots, n-1\} \to \{B_i/B_{i+1} \mid i = 0, \dots, m-1\},$$

että $A_i/A_{i+1} \cong f(A_i/A_{i+1})$ kaikilla $i = 0, \dots, n-1$.

Määritelmä 2.11 (Jonon hienonnus)**.** Jos ryhmällä G on sellaiset subnormaalit laskevat jonot

$$G = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_n \triangleright \cdots \quad \text{ja} \quad G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m \triangleright \cdots,$$

että jokaisella $i \geq 0$ pätee $H_i = N_j$ jollain j, jonoa (N_i) kutsutaan jonon (H_i) *hienonnukseksi*. Jokainen jonon (H_i) jäsen on siis myös jonon (N_i) jäsen.

Lause 2.12. Jos ryhmällä G on kaksi äärellistä subnormaalia laskevaa jonoa, niin niillä on isomorfiset hienonnukset.

Todistus. Oletetaan, että ryhmällä G on kaksi subnormaalia laskevaa jonoa, jotka ovat muotoa

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{1\} \quad \text{ja} \quad G = K_0 \triangleright K_1 \triangleright \cdots \triangleright K_m = \{1\}.$$

Muodostetaan jonoille isomorfiset hienonnukset. Asetetaan $H_{i,j} = (K_j \cap H_i)H_{i+1}$. Tällöin

$$H_i = H_{i,0} \geqslant H_{i,1} \geqslant \cdots \geqslant H_{i,m} = H_{i+1}.$$

Osoitetaan normaaliuskriteerin avulla, että aliryhmä $H_{i,j+1}$ on normaali ryhmässä $H_{i,j}$. Olkoon $x \in H_{i,j+1} = (K_{j+1} \cap H_i)H_{i+1}$ ja $g \in H_{i,j} = (K_j \cap H_i)H_{i+1}$. Tällöin $x = yh$ joillain $y \in (K_{j+1} \cap H_i)$ ja $h \in H_{i+1}$ ja $g = \tilde{g}\tilde{h}$ joillain $\tilde{g} \in (K_j \cap H_i)$ ja $\tilde{h} \in H_{i+1}$. Nyt

$$gxg^{-1} = \tilde{g}\tilde{h}yh\tilde{h}^{-1}\tilde{g}^{-1} = \tilde{g}\tilde{h}\tilde{g}^{-1}(\tilde{g}y\tilde{g}^{-1})\tilde{g}h\tilde{h}^{-1}\tilde{g}^{-1}.$$

Aliryhmä $K_{j+1} \cap H_i$ on normaali ryhmässä $K_j \cap H_i$, joten $y_2 := \tilde{g}y\tilde{g}^{-1} \in K_{j+1} \cap H_i$. Koska H_{i+1} on normaali ryhmässä H_i, niin $\tilde{h}_2 := \tilde{g}\tilde{h}\tilde{g}^{-1} \in H_{i+1}$ ja $k := \tilde{g}h\tilde{h}^{-1}\tilde{g}^{-1} \in H_{i+1}$. Näin ollen $\tilde{h}_2y_2 \in H_{i+1}(K_{j+1} \cap H_i)$, ja koska $H_{i+1}(K_{j+1} \cap H_i) = (K_{j+1} \cap H_i)H_{i+1}$, niin $\tilde{h}_2y_2 = y_3\tilde{h}_3$, missä $y_3 \in (K_{j+1} \cap H_i)$ ja $\tilde{h}_3 \in H_{i+1}$. Näin ollen siis

$$gxg^{-1} = \underbrace{\tilde{g}\tilde{h}\tilde{g}^{-1}}_{\tilde{h}_2}\underbrace{\tilde{g}y\tilde{g}^{-1}}_{y_2}\underbrace{\tilde{g}h\tilde{h}^{-1}\tilde{g}^{-1}}_{k} = y_3\tilde{h}_3k \in (K_{j+1} \cap H_i)H_{i+1},$$

joten $H_{i,j+1}$ on normaali ryhmässä $H_{i,j}$.

Ensimmäiselle jonolle saatiin siis hienonnus

$$\begin{aligned} G = H_0 \triangleright H_{0,1} \triangleright \cdots \triangleright H_{0,m-1} \triangleright H_1 \triangleright \cdots \triangleright H_{n-1} \\ \triangleright H_{n-1,1} \triangleright \cdots \triangleright H_{n-1,m-1} \triangleright H_n = \{1\}. \end{aligned}$$

Tämän jonon pituus on $nm + 1$.

Vastaavasti määritellään $K_{j,i} = (H_i \cap K_j)K_{j+1}$. Tällöin

$$K_j = K_{j,0} \geqslant K_{j,1} \geqslant \cdots \geqslant K_{j,n} = K_{j+1},$$

ja $K_{j,i+1}$ on normaali ryhmässä $K_{j,i}$. Toiselle jonolle saadaan siis hienonnus

$$\begin{aligned} G = K_0 \triangleright K_{0,1} \triangleright \cdots \triangleright K_{0,m-1} \triangleright K_1 \triangleright \cdots \triangleright K_{m-1,1} \\ \triangleright \cdots \triangleright K_{m-1,n-1} \triangleright K_m = \{1\}. \end{aligned}$$

Tämänkin jonon pituus on $mn + 1$.

Tutkitaan nyt ryhmää $H_{i,j}/H_{i,j+1}$. Alkuperäisten oletusten nojalla H_{i+1} on ryhmän H_i normaali aliryhmä. Koska lisäksi $K_{j+1} \cap H_i \triangleleft K_j \cap H_i < H_i$, niin lauseen 2.8 nojalla

$$\begin{aligned} H_{i,j}/H_{i,j+1} &= (K_j \cap H_i)H_{i+1}/(K_{j+1} \cap H_i)H_{i+1} \\ &\cong (K_j \cap H_i)/(K_{j+1} \cap H_i)((K_j \cap H_i) \cap H_{i+1}) \\ &= (K_j \cap H_i)/(K_{j+1} \cap H_i)(K_j \cap H_{i+1}). \end{aligned}$$

Tutkitaan nyt ryhmiä $K_{j,i}/K_{j,i+1}$. Ryhmä K_{j+1} on normaali ryhmän K_j aliryhmä ja $H_{i+1} \cap K_j \triangleleft H_i \cap K_j < K_j$, joten lauseen 2.8 nojalla

$$\begin{aligned} K_{j,i}/K_{j,i+1} &= (H_i \cap K_j)K_{j+1}/(H_{i+1} \cap K_j)K_{j+1} \\ &\cong (H_i \cap K_j)/(H_{i+1} \cap K_j)((H_i \cap K_j) \cap K_{i+1}) \\ &= (H_i \cap K_j)/(H_{i+1} \cap K_j)(H_i \cap K_{j+1}). \end{aligned}$$

Pitää vielä osoittaa, että $(K_{j+1} \cap H_i)(K_j \cap H_{i+1}) = (H_{i+1} \cap K_j)(H_i \cap K_{j+1})$. Kahden ryhmän G aliryhmän leikkauksena myös $H_i \cap K_{j+1}$ on ryhmän G aliryhmä. Koska lisäksi $H_i \cap K_{j+1} \subset H_i \cap K_j$, niin $H_i \cap K_{j+1}$ on ryhmän $H_i \cap K_j$ aliryhmä. Vastaavasti $H_{i+1} \cap K_j$ on ryhmän $H_i \cap K_j$ aliryhmä. Koska H_{i+1} on normaali ryhmässä H_i, niin $H_{i+1} \cap K_j$ on normaali ryhmässä $H_i \cap K_j$. Tällöin lauseen 2.2 nojalla

$(K_{j+1} \cap H_i)(K_j \cap H_{i+1})$ on ryhmän $H_i \cap K_j$ aliryhmä, mistä lauseen 2.1 nojalla seuraa, että $(K_{j+1} \cap H_i)(K_j \cap H_{i+1}) = (H_{i+1} \cap K_j)(H_i \cap H_{i+1})$.

Näin ollen $H_{i,j}/H_{i,j+1} \cong K_{j,i}/K_{j,i+1}$, joten jonojen hienonnukset ovat isomorfiset.

□

2.1.1 Karakteristiset aliryhmät

Määritellään seuraavaksi ryhmien karakteristiset aliryhmät. Nämä ovat sellaisia ryhmän aliryhmiä, jotka pysyvät samoina kuvattaessa ryhmää isomorfisesti itselleen.

Määritelmä 2.13 (Karakteristinen aliryhmä)**.** Olkoon G ryhmä, ja $K \subset G$. Aliryhmää K kutsutaan *karakteristiseksi aliryhmäksi,* jos kaikilla ryhmän G automorfismeilla $\phi \in \mathrm{Aut}(G)$, eli isomorfismeilla $\phi : G \to G$, pätee $\phi(K) = K$.

Lemma 2.14. Jokainen karakteristinen aliryhmä on myös normaali aliryhmä.

Todistus. Väite seuraa, kun osoitetaan, että konjugointi on ryhmän G automorfismi. Määritellään jokaiselle $g \in G$ konjugointikuvaus $\varphi_g \colon G \to G$, $h \mapsto ghg^{-1}$. Kuvaus φ_g on homomorfismi ja sillä on käänteiskuvauksena $\varphi_{g^{-1}}$. Näin ollen kuvaus φ_g on ryhmän G automorfismi jokaisella $g \in G$.

Jos H on ryhmän G karakteristinen aliryhmä, niin erityisesti $\varphi_g(H) = H$ jokaisella $g \in G$. Yhtäpitävästi siis $gHg^{-1} = H$ jokaisella $g \in G$, mistä seuraa, että H on normaali aliryhmä. □

Lause 2.15. Olkoon G ryhmä, jolla on aliryhmät H ja K, joille pätee lisäksi $K \leqslant H$. Jos H on karakteristinen ryhmässä G ja K karakteristinen ryhmässä H, niin K on karakteristinen ryhmässä G.

Todistus. Olkoon $\varphi : G \to G$ ryhmän G automorfismi. Tarkoituksena on osoittaa, että $\varphi(K) = K$. Aliryhmä H on karakteristinen ryhmässä G, joten $\varphi(H) = H$. Näin ollen $\varphi|_H : H \to \varphi(H)$ on ryhmän H automorfismi. Tällöin aliryhmän K karakteristisuudesta ryhmässä H seuraa, että $\varphi|_H(K) = K$. Kuitenkin $\varphi|_H(K) = \varphi(K)$, joten $\varphi(K) = K$. Näin ollen K on karakteristinen ryhmässä G. □

2.1.2 Äärellisen indeksin aliryhmät

Aliryhmän indeksillä tarkoitetaan vasempien sivuluokkien lukumäärää tämän aliryhmän suhteen. Jos aliryhmä on normaali, niin saadaan muodostettua tekijärakenne, joka on ryhmä. Tällöin erityisesti aliryhmän indeksi kertoo tekijäryhmän alkioiden lukumäärän.

Määritelmä 2.16. Ryhmän G aliryhmää H kutsutaan äärellisindeksiseksi ryhmässä G, jos $[G : H] < \infty$.

Määritelmä 2.17. Ryhmän G sanotaan olevan *melkein* *, jos sillä on jokin äärellisen indeksin aliryhmä H, jolla on ominaisuus *.

Esimerkki 2.18. Ryhmä voi olla esimerkiksi *melkein* vaihdannainen, jos sillä on jokin äärellisen indeksin aliryhmä, joka on vaihdannainen. Tyypillinen esimerkki *melkein* syklisestä ryhmästä on $\mathbb{Z} \times \mathbb{Z}_6$. Tällä ryhmällä on aliryhmä $\mathbb{Z} \cong \mathbb{Z} \times \{[0]_6\}$, joka on syklinen ja jonka indeksi on 6.

2.2 Kvasi-isometria

Seuraavissa tuloksissa oletetaan, että (X, d_X) ja (Y, d_Y) ovat metrisiä avaruuksia. Kvasi-isometria metristen avaruuksien välillä on kuvaus, joka ei säilytä etäisyyksiä täysin (vrt. isometria), mutta etäisyyksillä on joku yläraja. Kvasi-isometrioita tarvitaan osoittamaan, että ryhmien kasvu on ryhmän ominaisuus, joka ei riipu virittäjäjoukosta.

Määritelmä 2.19 (Karkea Lipschitz kuvaus)**.** Olkoon $f : X \to Y$ kuvaus. Jos on olemassa sellaiset $L \geq 1$ ja $C > 0$, että kaikilla $x, x' \in X$ pätee

$$d_Y(f(x), f(x')) \leq L d_X(x, x') + C,$$

niin kuvaus f on $(L, C)-$*karkea Lipschitz kuvaus.* Jos lisäksi kaikilla $x, x' \in X$ pätee

$$L^{-1} d_X(x, x') - C \leq d_Y(f(x), f(x')),$$

kuvausta f kutsutaan (L, C)-*kvasi-isometriseksi upotukseksi.*

Usein tällaisia kuvauksia f kutsutaan vain karkeiksi Lipschitz kuvauksiksi ja kvasi-isometrisiksi upotuksiksi, kun ei ole tarvetta tarkentaa vakioita L ja C.

Määritelmä 2.20. Olkoon $f : X \to Y$ ja $\bar{f} : Y \to X$ kuvauksia. Jos on olemassa sellainen vakio $C > 0$, että kaikilla $x \in X$ ja $y \in Y$ pätee

$$d_X(\bar{f} \circ f(x), x) \leq C \text{ ja } d_Y(f \circ \bar{f}(y), y) \leq C,$$

niin kuvaukset f ja $\bar{f}$ ovat toistensa *C-karkeat käänteiskuvaukset.* Erityisesti 0-karkeat käänteiskuvaukset ovat tavallisia käänteiskuvauksia.

Määritelmä 2.21 (Kvasi-isometriset avaruudet)**.** Kuvaus $f : X \to Y$ on *kvasi-isometria*, jos f on karkea Lipschitz ja sillä on karkea käänteiskuvaus, joka on myös karkea Lipschitz. Tarkemmin sanottuna f on (L, C)-kvasi-isometria avaruuksien X ja Y välillä, jos f on (L, C)-karkea Lipschitz, ja sille on olemassa sellainen (L, C)-karkea Lipschitz kuvaus $\bar{f} : Y \to X$, että f ja $\bar{f}$ ovat toistensa C-karkeita käänteiskuvauksia.

2.3 Lyhyet eksaktit jonot

Määritelmä 2.22. Olkoon G_i ryhmä jokaisella $i \in \mathbb{Z}$ ja olkoon $\varphi_j : G_j \to G_{j+1}$ ryhmähomomorfismi jokaisella $j \in \mathbb{Z}$. Jonoa

$$\cdots \to G_{n-1} \overset{\varphi_{\mathrm{n}-1}}{\to} G_n \overset{\varphi_{\mathrm{n}}}{\to} G_{n+1} \to \cdots,$$

jolle pätee $\operatorname{im} \varphi_i = \ker \varphi_{i+1}$ jokaisella $i \in \mathbb{N}$, kutsutaan *eksaktiksi jonoksi.*

Määritelmä 2.23. *Lyhyt eksakti jono* on eksakti jono, joka on muotoa

$$1 \to N \overset{\varphi}{\to} G \overset{\psi}{\to} H \to 1,$$

missä 1 tarkoittaa triviaalia ryhmää. Homomorfismi $1 \to N$ tarkoittaa triviaalia homomorfismia, $1 \mapsto 1_N$, ja homomorfismi $H \to 1$ homomorfismia $h \mapsto 1$.

Lemma 2.24. Olkoon

$$1 \to N \overset{\varphi}{\to} G \overset{\psi}{\to} H \to 1$$

jono ryhmiä. Tämä jono on lyhyt eksakti jono, jos ja vain jos φ on injektio, ψ on surjektio ja $\operatorname{im} \varphi = \ker \psi$.

Todistus. Oletetaan, että

$$1 \to N \overset{\varphi}{\to} G \overset{\psi}{\to} H \to 1$$

on lyhyt eksakti jono. Tällöin eksaktiuden nojalla $\ker \varphi = 1_N$ ja $\operatorname{im} \psi = 1$, eli φ on injektio ja ψ on surjetkio. Lisäksi eksaktiuden määritelmän nojalla $\operatorname{im} \varphi = \ker \psi$.

Oletetaan sitten, että φ on injektio, ψ on surjektio ja $\operatorname{im} \varphi = \ker \psi$. Ainoa ryhmähomomorfismi $1 \to N$ on triviaali homomorfismi $1 \mapsto 1_N$. Triviaalin homomorfismin kuva on neutraalialkio 1_N, mikä oletusten nojalla on kuvauksen φ ydin,

$\ker\varphi$. Näin ollen $1 \to N \to G$ on eksakti. Oletusten nojalla $\operatorname{im}\varphi = \ker\psi$, joten $N \to G \to H$ on eksakti. Lisäksi kuvauksen $H \to 1$ ydin on koko ryhmä H, mistä seuraa, että $G \to H \to 1$ on eksakti. Yhdistämällä nämä kohdat saadaan, että $1 \to N \to G \to H \to 1$ on lyhyt eksakti jono.

$\square$

Oletetaan, että N, G, H ovat ryhmiä ja että

$$1 \to N \xrightarrow{\varphi} G \xrightarrow{\psi} H \to 1$$

on lyhyt eksakti jono. Koska φ on injektio, niin $N \cong \varphi(N)$ eli N voidaan samastaa kuvansa, $\operatorname{im}\varphi$, kanssa. Ryhmä N voidaan siis ajatella ryhmän G aliryhmäksi. Ryhmä N on lisäksi normaali ryhmässä G, sillä eksaktiuden nojalla $N = \ker\psi$.

Lisäksi homomorfismi ψ on surjektio, joten ryhmien homomorfialauseen nojalla $G/\ker\psi \cong H$. Eksaktiuden nojalla $\operatorname{im}\varphi = \ker\psi$, joten $G/\operatorname{im}\varphi \cong H$. Näin ollen aiemman nojalla $G/N \cong H$, eli ryhmä H voidaan ajatella ryhmän G tekijäryhmänä ryhmän N suhteen.

Toisaalta, jos G on ryhmä ja N sen normaali aliryhmä, voidaan muodostaa lyhyt eksakti jono

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} G/N \to 1,$$

missä $\iota : N \hookrightarrow G$ on inkluusio ja $\pi : G \to G/N$ on tekijähomomorfismi.

Tässä työssä käytetään näitä samastuksia, kun todistuksissa käsitellään lyhyitä eksakteja jonoja. Jokainen ryhmän N alkio siis ajatellaan ryhmän G alkiona, ja ryhmän H alkiot ovat jotain tekijäryhmän G/N alkioita eli sivuluokkia gN.

Luku 3

Ryhmät ja aakkostot

3.1 Aakkostot ja sanat

Olkoon S joukko. Sen alkioita kutsutaan *kirjaimiksi* tai *symboleiksi*. Määritellään joukko $S^{-1} = \{a^{-1} \mid a \in S\}$ joukon S kirjainten *käänteiskirjaimiksi* tai *–symboleiksi*, ja muodostetaan tämän avulla *aakkosto* $S \cup S^{-1}$. *Sana* on jono aakkoston $S \cup S^{-1}$ kirjaimia. Sana on siis kirjainjono, joka on muotoa $a_1 \cdots a_n$, missä $a_i \in S \cup S^{-1}$. Voidaan myös määritellä *tyhjä sana*, jota merkitään yleisesti symbolilla 1. Aakkoston sanoille määritellään *pituus* sanan kirjainten lukumääränä. Sanaa kutsutaan *supistetuksi*, jos se ei sisällä peräkkäisiä kirjaimia aa^{-1} tai $a^{-1}a$. Muussa tapauksessa poistamalla tällaiset parit voidaan saada sanasta supistettu, ja yhden tällaisen parin poistoa kutsutaan *supistamiseksi*.

On yleistä kutsua aakkoston $S \cup S^{-1}$ sanoja vain joukon S sanoiksi. Käytetään vastaisuudessa aakkoston $S \cup S^{-1}$ sanojen joukolle merkintää $W(S)$ ja määritellään, että myös $1 \in W(S)$. Nyt joukkoon $W(S)$ voidaan määritellä ekvivalenssirelaatio seuraavasti: $w \sim w'$, jos sana w saadaan sanasta w' äärellisellä määrällä supistuksia ja niiden käänteisoperaatioita, eli lisäämällä jokin muotoa aa^{-1} tai $a^{-1}a$ oleva pari. Näin ollen relaatiot

$$ua_ia_i^{-1}v \sim uv \text{ ja } ua_i^{-1}a_iv \sim uv,$$

missä $u, v \in W(S)$, virittävät relaation $\sim$. Toisin sanoen ekvivalenssirelaatio $\sim$ on pienin ekvivalenssirelaatio, joka sisältää relaatiot

$$ua_ia_i^{-1}v \sim uv \text{ ja } ua_i^{-1}a_iv \sim uv.$$

Merkitään $F(S) = \{u \in W(S) \mid u \text{ on supistetussa muodossa}\}$.

Lemma 3.1. Jokainen sana $w \in W(S)$ on ekvivalentti yksikäsitteisen supistetun sanan kanssa.

Todistus. Todistetaan väite kahdessa osassa. Ensin osoitetaan supistetun sanan olemassaolo ja sitten sen yksikäsitteisyys. Molemmat todistetaan induktiolla tarkasteltavan sanan pituuden suhteen, mikä on yleinen keino todistaa aakkoston sanoihin liittyviä tuloksia.

Oletetaan siis, että $w \in W(S)$. Halutaan osoittaa, että on olemassa sellainen supistetussa muodossa oleva sana $v \in F(S)$, että $w \sim v$. Jos sanan w pituus on 0, niin $w = 1$, joka on jo supistetussa muodossa. Jos puolestaan sanan w pituus on 1, niin $w = a$, jollain $a \in S \cup S^{-1}$. Tämäkin on selvästi supistetussa muodossa. Oletetaan sitten, että jokaiselle n-pituiselle sanalle löytyy supistetussa muodossa oleva ekvivalentti sana, ja oletetaan, että sanan w pituus on $n+1$. Tällöin $w = a_1 \cdots a_n a_{n+1}$, missä $a_i \in S \cup S^{-1}$. Induktio-oletuksen nojalla on olemassa sellainen supistetussa muodossa oleva sana $v = b_1 \cdots b_k$, missä $b_j \in S \cup S^{-1}$, että $a_2 \cdots a_{n+1} \sim v$. Tällöin $w = a_1 \cdots a_n a_{n+1} \sim a_1 v$. Jos $a_1 \neq b_1^{-1}$, niin $a_1 v$ on supistetussa muodossa. Jos $a_1 = b_1^{-1}$, niin $a_1 v \sim b_2 \cdots b_k$, missä $b_2 \cdots b_k$ on oletusten nojalla supistetussa muodossa.

Näin ollen jokaiselle sanalle w on olemassa supistetussa muodossa oleva sana v, jolle pätee $w \sim v$.

Seuraavaksi halutaan näyttää, että supistetussa muodossa oleva sana on yksikäsitteinen, eli jos $v, w \in F(S)$ ja $v \sim w$, niin $v = w$. Ennen kuin lähdetään tätä suoraan todistamaan, määritellään seuraavanlainen apufunktio: jokaista aakkoston $S \cup S^{-1}$ kirjainta a kohti määritellään funktio $L_a : F(S) \to F(S)$ kaavalla

$$L_a(b_1 \cdots b_k) = \begin{cases} ab_1 \cdots b_k, & \text{jos } a \neq b_1^{-1} \\ b_2 \cdots b_k, & \text{jos } a = b_1^{-1} \end{cases}$$

kun $b_1 \cdots b_k \in F(S)$. Tämä funktio on hyvin määritelty, sillä määritelmästä johtuen $L_a(b_1 \cdots b_k)$ on supistetussa muodossa ja yksikäsitteinen. Nyt jokaista sanaa $w = a_1 \cdots a_n$ kohti määritellään $L_w = L_{a_1} \circ \cdots \circ L_{a_n}$ ja $L_1 = \mathrm{id}$ tyhjälle sanalle 1.

Oletetaan, että $a \in S \cup S^{-1}$. Kaikilla $b_1 \cdots b_k \in F(S)$ pätee $L_a \circ L_{a^{-1}}(b_1 \cdots b_k) = b_1 \cdots b_k = \mathrm{id}(b_1 \cdots b_k)$, eli $L_a \circ L_{a^{-1}} = \mathrm{id}$. Olkoon sitten $v, w \in W(S)$ ja oletetaan, että $v \sim w$. Riittää tarkastella sellaista tilannetta, että sana w saadaan sanasta u supistamalla jokin muotoa aa^{-1} oleva pari. Jatkamalla induktiivisesti tällaisten parien supistamista saadaan myös yleinen tilanne $u \sim w$ todistettua. Oletetaan siis, että $v = uaa^{-1}u'$ kun $w = uu'$ joillain $u, u' \in W(S)$ ja $a \in S \cup S^{-1}$. Tällöin $L_v = L_u \circ L_a \circ L_{a^{-1}} \circ L_{u'} = L_w$. Siis jos $v \sim w$, niin $L_v = L_w$.

Osoitetaan sitten jälleen induktiolla sanan pituuden suhteen, että jos sana w on supistetussa muodossa, niin $L_w(1) = w$. Tämä pätee kun sanan w pituus on 0 tai 1, sillä $L_1(1) = 1$ ja $L_a(1) = a$ kaikilla $a \in S \cup S^{-1}$. Oletetaan sitten, että tämä pätee kaikilla supistetussa muodossa olevilla n-pituisilla sanoilla ja oletetaan, että $w \in F(S)$ on $(n+1)$-pituinen sana. Nyt $w = au$, jollain $u \in F(S)$ ja $a \in S \cup S^{-1}$. Induktio-oletuksen nojalla $u = L_u(1)$ ja näin ollen voidaan päätellä, että $L_w(1) = L_a \circ L_u(1) = L_a(u) = au = w$.

Kaiken tämän jälkeen ollaan valmiita osoittamaan yksikäsitteisyys, mikä sujuu näiden apupohdintojen avulla suoraviivaisesti. Olkoot $v, w \in F(S)$ sellaiset, että $v \sim w$. Tällöin $v = L_v(1) = L_w(1) = w$, mikä todistaa yksikäsitteisyyden.

Näin ollen jokainen sana $w \in W(S)$ on ekvivalentti yksikäsitteisen supistetussa muodossa olevan sanan kanssa. $\square$

3.2 Vapaat ryhmät ja relaatiot

3.2.1 Vapaat ryhmät

Oletetaan, että S on joukko. Olkoon $F(S)$ aakkoston $S \cup S^{-1}$ supistetussa muodossa olevien sanojen joukko, eli $F(S) \subset W(S)$ kuten luvussa 3.1. Joukkoon $F(S)$ voidaan määritellä laskutoimitus $*$ seuraavasti. Olkoot $w, w' \in F(S)$. Tällöin $w * w'$ on se yksikäsitteinen supistetussa muodossa oleva aakkoston $S \cup S^{-1}$ sana, joka on ekvivalentti sanan ww' kanssa. Siis $w * w' = v$, missä $v \in F(S)$ ja $ww' \sim v$ joukossa $W(S)$. Tämä on hyvin määritelty laskutoimitus, sillä lemman 3.1 nojalla laskutoimituksen tulos on olemassa ja yksikäsitteinen.

Tarkastellaan laskutoimitusta $*$ tarkemmin. Jotta pari $(F(S), *)$ olisi ryhmä, joukon $F(S)$ täytyy sisältää neutraalialkio laskutoimitukselle $*$ ja käänteisalkiot jokaiselle sanalle $w \in F(S)$ laskutoimituksen $*$ suhteen. Tämän lisäksi laskutoimituksen $*$ on oltava liitännäinen joukossa $F(S)$.

Lemma 3.2. Laskutoimituksen $*$ neutraalialkio on tyhjä sana 1, joka sisältyy joukkoon $F(S)$. Joukko $F(S)$ sisältää kaikkien alkioidensa käänteisalkiot laskutoimituksen $*$ suhteen, eli jos $w \in F(S)$, niin $w^{-1} \in F(S)$.

Todistus. Jos $w \in F(S)$, eli w on supistetussa muodossa oleva sana, niin $w * 1 = w$ ja $1 * w = w$. Koska on määritelty, että $1 \in F(S)$, voidaan päätellä laskutoimituksen $*$ neutraalialkion sisältyvän joukkoon $F(S)$.

Jos $a_1 \cdots a_n \in F(S)$ sana, niin $(a_1 \cdots a_n) * (a_n^{-1} \cdots a_1^{-1}) = 1$ ja $(a_n^{-1} \cdots a_1^{-1}) * (a_1 \cdots a_n) = 1$. Koska $a_1 \cdots a_n$ on supistetussa muodossa oleva sana, niin myös sana $a_n^{-1} \cdots a_1^{-1}$ on supistetussa muodossa eli $a_n^{-1} \cdots a_1^{-1} \in F(S)$. Näin ollen joukko $F(S)$ sisältää alkioidensa käänteisalkiot laskutoimituksen $*$ suhteen. □

Lemma 3.3. Laskutoimitus $*$ on liitännäinen joukossa $F(S)$.

Todistus. Määritellään kuvaus $r \colon W(S) \to F(S)$, joka liittää jokaiseen aakkoston $S \cup S^{-1}$ sanaan $w \in W(S)$ sen yksikäsitteisen supistetussa muodossa olevan sanan $w' \in F(S)$, jolle pätee $w \sim w'$. Kuvaus r siis liittää jokaiseen sanaan $w \in W(S)$ sen supistetun muodon. Tämä kuvaus on hyvin määritelty lemman 3.1 nojalla.

Nyt kaikilla sanoilla $v, w \in W(S)$ pätee $r(v)w \sim vw \sim vr(w)$, joten $r(r(v)w) = r(vw) = r(vr(w))$. Lisäksi sanoilla $v, w \in F(S)$ pätee $v * w = r(vw)$. Näin ollen kaikilla sanoilla $v, w, z \in F(S)$ pätee

$$\begin{aligned}(v * w) * z &= r((v * w)z) = r(r(vw)z) = r(vwz) \\ &= r(vr(wz)) = r(v(w * z)) = v * (w * z),\end{aligned}$$

eli laskutoimitus $*$ on liitännäinen joukossa $F(S)$. □

Lemmojen 3.2 ja 3.3 nojalla pari $(F(S), *)$ on ryhmä.

Määritelmä 3.4. Pari $(F(S), *)$ on ryhmä, ja sitä kutsutaan *joukon S vapaaksi ryhmäksi.*

Lause 3.5 (Vapaiden ryhmien universaaliominaisuus)**.** Oletetaan, että X on joukko ja G on ryhmä. Jokainen kuvaus $\varphi : X \to G$ voidaan yksikäsitteisesti laajentaa homomorfismiksi $\Phi : F(X) \to G$.

Todistus. Oletetaan, että X on joukko, G on ryhmä ja $\varphi : X \to G$ kuvaus. Ajatellaan tässä ryhmän G laskutoimitusta kertolaskuksi, ja käytetään alkioiden $g, h \in G$ tulolle merkintää gh. Kuvaus φ voidaan laajentaa kuvaukseksi koko aakkostolta $X \cup X^{-1}$ valitsemalla $\varphi(a^{-1}) = \varphi(a)^{-1}$ jokaisella $a \in X$.

Osoitetaan ensin, että homomorfismi $\Phi : F(X) \to G$ on olemassa. Homomorfismille Φ täytyy päteä $\Phi(w * w') = \Phi(w)\Phi(w')$ kaikilla $w, w' \in F(X)$ ja lisäksi $\Phi(a) = \varphi(a)$ kaikilla $a \in X \cup X^{-1}$, jotta se olisi kuvauksen φ laajennos.

Määritellään siis $\Phi(a) = \varphi(a)$ kaikilla $a \in X \cup X^{-1}$ ja $\Phi(1) = 1_G$. Tämän avulla voidaan määrittää kaikille sanoille $w = a_1 \cdots a_n \in F(X)$ kuvaksi $\Phi(w) = \varphi(a_1) \cdots \varphi(a_n)$. Näytetään sitten, että $\Phi(w * w') = \Phi(w)\Phi(w')$. Jos sana ww' on supistetussa muodossa, väite seuraa suoraviivaisesti. Oletetaan siis, että ww' ei ole supistetussa muodossa. Yksinkertaisimmassa tapauksessa tämä tarkoittaa, että $w = a_1 \cdots a_n b$ ja $w' = b^{-1} a_1' \cdots a_k'$, jolloin $ww' \sim a_1 \cdots a_n a_1' \cdots a_k'$, eli erityisesti $w * w' = a_1 \cdots a_n a_1' \cdots a_k'$. Nyt

$$\begin{aligned}
\Phi(w * w') &= \Phi(a_1 \cdots a_n a_1' \cdots a_k') = \varphi(a_1) \cdots \varphi(a_n)\varphi(a_1') \cdots \varphi(a_k') \\
&= \varphi(a_1) \cdots \varphi(a_n)\ 1_G\ \varphi(a_1') \cdots \varphi(a_k') \\
&= \varphi(a_1) \cdots \varphi(a_n)\varphi(b)\varphi(b)^{-1}\varphi(a_1') \cdots \varphi(a_k') \\
&= \Phi(w)\Phi(w').
\end{aligned}$$

Yleisessä tapauksessa, jos ww' ei ole supistetussa muodossa, täytyy päteä $w = a_1 \cdots a_i \cdots a_n$ ja $w' = a_n^{-1} \cdots a_i^{-1} b_1 \cdots b_k$ jollain $i \geq 2$. Tässä tapauksessa voidaan menetellä kuten aiemmassa tapauksessa useamman kerran peräkkäin, jolloin saadaan $\Phi(w * w') = \Phi(w)\Phi(w')$. Siis Φ on homomorfismi, joka on kuvauksen φ laajennos.

Osoitetaan sitten, että tämä homomorfismi on yksikäsitteinen. Olkoon siis $\Psi : F(X) \to G$ homomorfismi, jolle pätee $\Psi(a) = \varphi(a)$ kaikilla $a \in X$. Nyt kaikilla sanoilla $w = a_1 \cdots a_n \in F(X)$ pätee $\Psi(w) = \Psi(a_1) \cdots \Psi(a_n) = \varphi(a_1) \cdots \varphi(a_n) = \Phi(w)$. Näin ollen homomorfismi Φ on yksikäsitteinen. $\square$

3.2.2 Ryhmän relaatiot ja esitys

Määritelmä 3.6 (Normaali sulkeuma)**.** Olkoon G ryhmä ja $R \subset G$. Pienintä ryhmän G normaalia aliryhmää, joka sisältää joukon R, kutsutaan joukon R *normaaliksi sulkeumaksi* ja merkitään $\langle\langle R \rangle\rangle$.

Lemma 3.7. Olkoon G ryhmä ja $R \subset G$. Tällöin joukon R normaalin sulkeuman $\langle\langle R \rangle\rangle$ virittäjäjoukko on $\{grg^{-1} \mid r \in R, g \in G\}$.

Todistus. Olkoon K joukon $S = \{grg^{-1} \mid r \in R, g \in G\}$ virittämä ryhmän G aliryhmä. Olkoon $k \in K$. Tällöin $k = \Pi_{i=1}^{n} g_i r_i g_i^{-1}$. Näin ollen, jos $h \in G$, niin $hkh^{-1} = \Pi_{i=1}^{n} h g_i r_i g_i^{-1} h_i^{-1} \in K$, joten normaaliuskriteerin nojalla K on normaali ryhmässä G. Koska lisäksi $R \subset K$, niin normaalin sulkeuman määritelmän nojalla $\langle\langle R \rangle\rangle \subset K$.

Jos $r \in R$ ja $g \in G$, niin normaaliuskriteerin nojalla $grg^{-1} \in \langle\langle R \rangle\rangle$, eli $S \subset \langle\langle R \rangle\rangle$. Näin ollen $K \subset \langle\langle R \rangle\rangle$, sillä määritelmän nojalla K on pienin ryhmän G aliryhmä, joka sisältää joukon S.

Näin ollen joukon R normaali sulkeuma $\langle\langle R \rangle\rangle$ on joukon $\{grg^{-1} \mid r \in R, g \in G\}$ virittämä. $\square$

Olkoon G ryhmä ja S sen virittäjäjoukko. Vapaiden ryhmien universaaliominaisuuden, lause 3.5, nojalla saadaan, että inkluusiokuvaus $\iota : S \hookrightarrow G$ voidaan laajentaa yksikäsitteisesti homomorfismiksi $\pi_S : F(S) \to G$.

Määritelmä 3.8 (Ryhmän relaatiot)**.** Homomorfismin $\pi_S : F(S) \to G$ ytimen $\ker \pi_S$ alkioita kutsutaan ryhmän G *relaatioiksi* virittäjäjoukon S suhteen.

Huomautus. Joukko S on ryhmän G virittäjäjoukko, joten jos $g \in G$, niin $g = s_1 \cdots s_n$, missä $s_i \in S$ tai $s_i^{-1} \in S$ jokaisella i. Voidaan olettaa, että g on sievennetyssä muodossa, joten $s_1 \cdots s_n \in F(S)$. Nyt $\pi_S(s_1 \cdots s_n) = \iota(s_1) \cdots \iota(s_n) = s_1 \cdots s_n = g$. Näin ollen π_S on surjektio.

Määritelmä 3.9 (Ryhmän esitys)**.** Olkoon $R \subset F(S)$ sellainen, että $\ker \pi_S = \langle\langle R \rangle\rangle$. Tällöin joukon R alkioita kutsutaan ryhmän G *määrittäviksi relaatioiksi*. Ryhmien homomorfialauseen nojalla $G \cong F(S)/\langle\langle R \rangle\rangle$. Paria (S, R) kutsutaan *ryhmän G esitykseksi* ja merkitään $\langle S \mid R \rangle$. Jos sekä S että R ovat äärellisiä joukkoja, niin esitystä $\langle S \mid R \rangle$ kutsutaan *äärelliseksi*.

Alla oleva kaavio havainnollistaa ryhmän esitystä ja konstruktiota. Inkluusiokuvauksesta $\iota : S \hookrightarrow G$ saadaan vapaiden ryhmien universaaliominaisuuden nojalla yksikäsitteinen surjektiivinen homomorfismi $\pi_S : F(S) \to G$. Jos $\langle\langle R \rangle\rangle = \ker \pi_S$, niin ryhmien homomorfialauseen nojalla saadaan isomorfismi $\overline{\pi}_S : F(S)/\langle\langle R \rangle\rangle \to G$, jolle pätee $\pi_S = \overline{\pi}_S \circ \pi$, missä $\pi : F(S) \to F(S)/\langle\langle R \rangle\rangle$ on tekijähomomorfismi. Tällöin alla oleva kaavio kommutoi:

$$\begin{tikzcd}
F(S) \arrow[r, "\pi_S"] \arrow[d, "\pi"] & G \\
F(S)/\langle\langle R \rangle\rangle \arrow[ur, "\overline{\pi}_S"] &
\end{tikzcd}$$

Huomautus. Jos ryhmällä G on esitys $\langle S \mid R \rangle$, niin jokainen ryhmän G alkio g voidaan kirjoittaa aakkoston $S \cup S^{-1}$ sanana: jos $g \in G$, niin kuvauksen π_S surjektiivisuuden nojalla on olemassa aakkoston $S \cup S^{-1}$ sana $w = s_1 \cdots s_n$, jolle pätee $\pi_S(w) = g$. Toisaalta $\pi_S(w) = \iota(s_1) \cdots \iota(s_n)$, joten $g = s_1 \cdots s_n$.

Huomautus. Oletetaan, että ryhmällä G on esitys $\langle S \mid R\rangle$, ja olkoon w aakkoston $S \cup S^{-1}$ (supistetussa muodossa oleva) sana. Tällöin *sana w on ekvivalentti neutraalialkion kanssa ryhmässä G*, toisin sanoen $\pi_S(w) = 1_G$, jos ja vain jos

$$w = \prod_{i=1}^{n} u_i r_i u_i^{-1},$$

missä $u_i \in F(S)$ jokaisella i. Tämä ominaisuus havaitaan seuraavasti.

Jos $w \in F(S)$ sellainen, että $\pi_S(w) = 1_G$, niin $\overline{\pi}_S \circ \pi(w) = 1_G$. Koska $\overline{\pi}_S$ on isomorfismi, tästä seuraa, että $w \in \langle\langle R\rangle\rangle$. Näin ollen lauseen 3.7 nojalla sana w on äärellinen tulo relaatioiden $r_i \in R$ konjugaatteja.

Toisaalta, jos oletetaan, että $w = \prod_{i=1}^{n} u_i r_i u_i^{-1}$, missä $u_i \in F(S)$ jokaisella i, niin $w \in \langle\langle R\rangle\rangle$, joten

$$\pi_S(w) = \overline{\pi}_S \circ \pi(w) = 1_G.$$

Esimerkki 3.10. Tyypillisenä esimerkkinä ryhmien esityksestä voidaan antaa kahden virittäjän vaihdannainen ryhmä G, jolla on esitys $\langle a, b \mid aba^{-1}b^{-1}\rangle$.

Seuraavaksi käsitellään äärellisiin esityksiin liittyviä ominaisuuksia. Ensimmäisenä todetaan, että äärellinen esitys ei riipu virittäjäjoukosta. Sen jälkeen esiteltävä lause tulee tarpeen, kun osoitetaan, että myöhemmin esiteltävillä *polysyklisillä* ryhmillä on äärellinen esitys.

Lausetta 3.11 ei todisteta tässä, mutta se löytyy kirjasta [2, proposition 7.28].

Lause 3.11. Oletetaan, että ryhmällä G on äärellinen esitys $\langle S \mid R\rangle$, ja olkoon $\langle X \mid T\rangle$ ryhmän G esitys, missä virittäjäjoukko X on äärellinen. Tällöin on olemassa sellainen äärellinen $T_0 \subset T$, että $\langle X \mid T_0\rangle$ on ryhmän G esitys.

Lause 3.12. Jos N on ryhmän G normaali aliryhmä, ja sekä ryhmällä N että ryhmällä G/N on äärellinen esitys, niin myös ryhmällä G on äärellinen esitys.

Todistus. Olkoon $\langle X \mid r_1, \dots, r_k\rangle$ ryhmän N äärellinen esitys, ja olkoon Y sellainen ryhmän G äärellinen osajoukko, että $\langle \bar{Y} \mid \bar{p_1}, \dots, \bar{p}_m\rangle$, missä $\bar{Y} = \{yN \mid y \in Y\}$, on ryhmän G/N äärellinen esitys. Lauseen 3.11 nojalla Y on olemassa.

Merkitään $R = \{r_1, \dots, r_k\}$ ja $\bar{P} = \{\bar{p_1}, \dots, \bar{p}_m\}$. Koska $N = \langle X \mid R\rangle$, niin määritelmän nojalla $N \cong F(X)/\langle\langle R\rangle\rangle$, missä $\langle\langle R\rangle\rangle = \ker \pi_X$ ja $\pi_X : F(X) \to N$. Vastaavasti $G/N \cong F(\bar{Y})/\langle\langle \bar{P}\rangle\rangle$, missä $\langle\langle \bar{P}\rangle\rangle = \ker \pi_{\bar{Y}}$ ja $\pi_{\bar{Y}} : F(\bar{Y}) \to G/N$.

Merkitään $S = X \cup Y$ ja osoitetaan, että S on ryhmän G äärellinen virittäjäjoukko. Osajoukko S on äärellinen, sillä sekä X että Y ovat äärellisiä. Koska X on aliryhmän N virittäjäjoukko, riittää tarkastella alkioita $g \notin N$. Tällöin ryhmässä G/N pätee $gN \neq N$ ja $gN = y_1^{k_1} \cdots y_l^{k_l} N$, missä $y_i \in Y$ ja $k_i \in \mathbb{Z}$. Tästä seuraa, että $(y_1^{k_1} \cdots y_l^{k_l})^{-1} g \in N$, joten $(y_1^{k_1} \cdots y_l^{k_l})^{-1} g = x_1^{m_1} \cdots x_n^{m_n}$, missä $x_i \in X$ ja $m_i \in \mathbb{Z}$, sillä joukko X virittää ryhmän N. Nyt $g = y_1^{k_1} \cdots y_l^{k_l} x_1^{m_1} \cdots x_n^{m_n}$, joten joukko S virittää ryhmän G.

Olkoon $i_S : S \to G$ inkluusio. Vapaiden ryhmien universaaliominaisuuden nojalla on olemassa yksikäsitteinen homomorfismi $\pi_S : F(S) \to G$, joka laajentaa kuvausta i_S. Koska joukko S on ryhmän G äärellinen virittäjäjoukko, homomorfismi π_S on sujektio. Näin ollen pätee $G \cong F(S)/\ker \pi_S$. Halutaan löytää sellainen äärellinen joukko $T \subset F(S)$ sanoja, että $\ker \pi_S = \langle\langle T \rangle\rangle$.

Tutkitaan ryhmän G/N relaatioita $\bar{p}_j$. Koska joukko $\bar{Y}$ virittää ryhmän G/N, niin $\bar{p}_j = y_1 N \cdots y_n N$ joillain $y_i N \in \bar{Y} \cup \bar{Y}^{-1}$. Sana $\bar{p}_j$ on ryhmän G/N relaatio, eli $\pi_{\bar{Y}}(\bar{p}_j) = 1_{G/N}$, joten $y_1 \cdots y_n N = N$. Näin ollen alkio $y_1 \cdots y_n \in N$. Kuvaus π_X on surjektio, joten on olemassa jokin sana $u_j \in F(X)$, jolla $\pi_X(u_j) = y_1 \cdots y_n$. Toisaalta $p_j = y_1 \cdots y_n$ on sellainen aakkoston $S \cup S^{-1}$ sana, jolla $\pi_S(p_j) = y_1 \cdots y_n$. Näin ollen aakkoston $S \cup S^{-1}$ sanoille pätee $\pi_S(p_j) = \pi_S(u_j)$. Erityisesti $u_j^{-1} p_j \in \ker \pi_S$.

Aliryhmä N on normaali ryhmässä G, joten $yxy^{-1} \in N$ ja $y^{-1}xy \in N$ jokaisella $x \in X$ ja $y \in Y$. Näin ollen on olemassa aakkoston $X \cup X^{-1}$ sanat v_{xy} ja w_{xy}, joilla $\pi_S(v_{xy}) = \pi_X(v_{xy}) = yxy^{-1}$ ja $\pi_S(w_{xy}) = \pi_X(w_{xy}) = y^{-1}xy$. Näin ollen aakkoston $S \cup S^{-1}$ sanoille v_{xy} ja yxy^{-1} pätee $v_{xy}^{-1} yxy^{-1} \in \ker \pi_S$. Vastaavasti sanoille w_{xy} ja $y^{-1}xy$ pätee $w_{xy}^{-1} y^{-1}xy \in \ker \pi_S$.

Olkoon $T \subset F(S)$ se äärellinen osajoukko, joka koostuu sanoista

(1) r_i, $1 \leq i \leq k$

(2) $u_j^{-1} p_j$, $1 \leq j \leq m$

(3) $v_{xy}^{-1} yxy^{-1}$, $w_{xy}^{-1} y^{-1}xy$, jokaisella $x \in X$, $y \in Y$,

ja olkoon K pienin ryhmän $F(S)$ normaali aliryhmä, joka sisältää joukon T, eli $K = \langle\langle T \rangle\rangle$. Aliryhmä K sisältyy aliryhmään $\ker \pi_S$, joten homomorfismi π_S määrittää surjektiivisen homomorfismin $\varphi : F(S)/K \to G$. Tarkoituksena on osoittaa, että φ on myös injektio, jolloin $F(S)/K \cong G$.

Olkoon siis $wK \in \ker \varphi$, missä $w \in F(S)$ on aakkoston $S \cup S^{-1}$ sana. Koska konjugaateille yxy^{-1} ja $y^{-1}xy$ pätee $yxy^{-1}K = v_{xy}K$ ja $y^{-1}xyK = w_{xy}K$, lisäämällä sanaan w tarvittaessa jokin muotoa yy^{-1} tai $y^{-1}y$ oleva kirjainpari, alkio wK voidaan kirjoittaa muodossa $w_X w_Y K$. Tässä w_X on aakkoston $X \cup X^{-1}$ sana ja w_Y on aakkoston $Y \cup Y^{-1}$ sana.

Olkoon $\pi : G \to G/N$ tekijähomomorfismi aliryhmän N suhteen. Koska oletuksen nojalla $wK \in \ker \varphi$, niin

$$\pi \circ \varphi(wK) = \pi \circ \varphi(w_X w_Y K) = \pi(\varphi(w_X K)\varphi(w_Y K)) = \pi(\varphi(w_Y K)) = 1_{G/N},$$

sillä $\varphi(w_X K) = \pi_S(w_X) \in N$.

Näin ollen sana $w_Y = y_1 \cdots y_l$ on sellainen, että $\pi_S(w_Y) = y_1 \cdots y_l \in N$. Tästä seuraa, että $w_{\bar{Y}} = y_1 N \cdots y_l N \in \langle\langle \bar{P} \rangle\rangle$. Erityisesti sana $w_{\bar{Y}}$ on äärellinen tulo sanojen $\bar{p}_j$ konjugaatteja, jolloin sana w_Y on äärellinen tulo sanojen p_j konjugaatteja. Koska $p_j K = u_j K$, niin $w_Y K$ on äärellinen tulo sanojen $u_j K$ konjugaatteja. Jälleen, koska $yxyK = v_{xy}K$ ja $y^{-1}xyK = w_{xy}K$, saadaan, että $w_Y K = v_X K$, missä v_X on jokin aakkoston $X \cup X^{-1}$ sana.

On osoitettu, että $wK = w_X v_X K$, mistä seuraa, että $\varphi(wK) = \varphi(w_X v_X K) = \pi_S(w_X v_X) = 1_G$, joten aakkoston $X \cup X^{-1}$ sana $w_X v_X$ on äärellinen tulo sanojen $r_i \in T$ konjugaatteja. Tällöin $w_X v_X \in K$, sillä $r_i \in K$ ja ryhmä K on normaali ryhmässä $F(S)$. Tällöin erityisesti $w_X v_X K = K$, joten $wK = w_X v_X K = K$.

On osoitettu, että $\ker \varphi = \{K\}$, joten kuvaus φ on injektio. Näin ollen φ on isomorfismi. Tällöin $F(S)/K \cong G \cong F(S)/\ker \pi_S$, joten $\ker \pi_S = K$. Ryhmä $\ker \pi_S$ on siis pienin normaali aliryhmä, joka sisältää relaatiot T. Näin ollen määritelmän nojalla $\langle S \mid T \rangle$ on ryhmän G äärellinen esitys. $\square$

Luku 4

Geometrisia käsitteitä

Tässä luvussa määritellään ryhmien *Cayley graafit*, joiden avulla ryhmiä voidaan käsitellä geometrisina objekteina. Äärellisesti viritettyyn ryhmään määritellään metriikka sen Cayley graafin avulla, jolloin ryhmistä saadaan topologisia avaruuksia. Tätä metriikkaa kutsutaan *sanametriikaksi*.

4.1 Graafit

Tässä alaluvussa on tämän tutkielman päälähteen, kirjan [2], lisäksi käytetty lähteenä kirjaa [11], ja erityisesti sen graafeja koskevia tuloksia.

Määritelmä 4.1. *Suuntaamaton graafi* Γ koostuu

- joukosta V, joka sisältää graafin *solmut*
- joukosta E, joka sisältää graafin *kaaret*
- kuvauksesta ι, joka on määritelty kaarien joukosta E solmujen joukon V yhden ja kahden kokoisiin osajoukkoihin. Jos $\iota(e) = \{u, v\}$ jollain kaarella $e \in E$ ja joillain solmuilla $u, v \in V$, sanotaan, että solmut u ja v ovat kaaren e päätepisteitä. Tällöin solmut u ja v ovat *vierekkäisiä*. Jos puolestaan $\iota(e) = \{u\}$, kun $e \in E$ ja $u \in V$, niin e on kaari solmusta u itseensä.

Graafeja kutsutaan myös *verkoiksi*.

Tutkitaan tarkemmin kuvausta ι. Jos $\iota(e) = \{u, v\}$, eli solmut u ja v ovat kaaren e päätepisteitä, niin kaarelle voidaan antaa suunta valitsemalla solmuista toinen kaaren *alkupisteeksi* ja toinen kaaren *päätepisteeksi*. Määritellään alku- ja päätepistekuvaukset $o : E \to V$ ja $t : E \to V$ niin, että $o(e)$ kuvautuu kaaren e alkupusteelle ja $t(e)$ kuvautuu kaaren e päätepisteelle.

Määritelmä 4.2. *Suunnattu graafi* Γ koostuu

- joukosta V, joka sisältää graafin *solmut*
- joukosta E, joka sisältää graafin *kaaret*
- parista kuvauksia $o : E \to V$ ja $t : E \to V$, missä kuvaus o (origin) kertoo kaaren e alkupisteen ja kuvaus t (tail) kertoo kaaren e päätepisteen. Tätä paria kuvauksia kutsutaan *graafin suuntaukseksi*.

Määritelmä 4.3. Olkoon Γ (suuntaamaton tai suunnattu) graafi. Solmun $v \in V$ *asteeksi* kutsutaan solmusta v lähtevien kaarien lukumäärää. Jos solmusta v lähtee kaari itseensä, se lasketaan kahdesti. Graafin Γ *asteeksi* tai *valenssiksi* kutsutaan sen solmujen asteiden supremumia.

Määritelmä 4.4. Olkoon Γ suuntaamaton graafi. Äärellistä ja järjestettyä jonoa $e_1, \ldots, e_n$, missä $e_i \in E$ ovat sellaisia, että $\iota(e_i) = \{v_i, v_{i+1}\}$ ja $\iota(e_i) \cap \iota(e_{i+1}) \neq \emptyset$, $1 \leq i \leq n$, kutsutaan *kaaripoluksi* graafissa Γ. Tässä $e_1, \ldots, e_n$ on solmujen v_1 ja v_{n+1} välinen kaaripolku. Kaaripolun *pituus* on sen kaarien pituuksien summa. Graafi Γ on *yhtenäinen*, jos jokaisen kahden solmun v ja w välillä on jokin kaaripolku.

4.2 Ryhmät geometrisina objekteina

Tässä alaluvussa ryhmistä muodostetaan geometrisia objekteja niiden Cayley graafien avulla. Äärellisesti viritetyn ryhmän G Cayley graafin solmut ovat ryhmän alkiot ja kaaret koostuvat niistä pareista ryhmän alkioita, jotka saadaan toisistaan jollakin virittäjäalkiolla tai virittäjäalkion käänteisalkiolla.

4.2.1 Cayley graafit

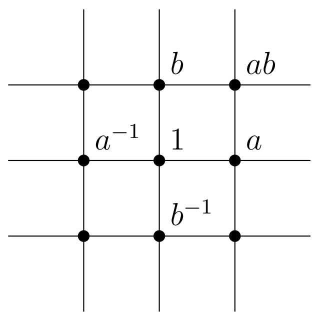
Määritelmä 4.5. Olkoon G ryhmä ja S sen virittäjäjoukko. Ryhmän G *Cayley graafi* joukon S suhteen on suuntaamaton graafi $\mathrm{Cayley}(G, S)$, jossa

- solmujen joukko on G

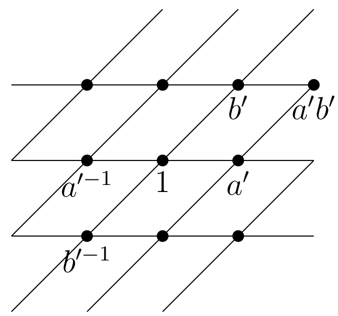
- kaarien joukko koostuu alkioista e, joilla $\iota(e) = \{g, h\}$, missä $h = gs$ jollain $s \in S$ tai $s^{-1} \in S$.

Cayley graafit muodostetaan virittäjäjoukon S suhteen, mistä johtuu, että eri virittäjäjoukot voivat antaa samalle ryhmälle erinäköiset Cayley graafit.

Tyypillisenä esimerkkinä mainitaan ryhmä $\mathbb{Z} \times \mathbb{Z}$, jolle voidaan piirtää Cayley graafit esimerkiksi virittäjien $\{a = (1,0), b = (0,1)\}$ tai virittäjien $\{a' = (1,0), b' = (1,1)\}$ suhteen.



Kuva 4.1: Cayley graafi virittäjien $\{a, b\}$ suhteen



Kuva 4.2: Cayley graafi virittäjien $\{a', b'\}$ suhteen

Lemma 4.6. Jokainen ryhmä G toimii itseensä transitiivisesti. Erityisesti tästä seuraa, että ryhmän G Cayley graafi jonkin virittäjäjoukon S suhteen on yhtenäinen.

Todistus. Olkoon G ryhmä ja $g, h \in G$. Halutaan näyttää, että ryhmän toiminta itseensä vasemmalta on transtiivista, eli $h = g'g$ jollain $g' \in G$. Selvästi tämä pätee, sillä $h = (hg^{-1})g = g'g$ valinnalla $g' = hg^{-1} \in G$.

Oletetaan sitten, että ryhmällä G on virittäjäjoukko S. Tällöin g on muotoa $s_1 \cdots s_n$ ja h on muotoa $s'_1 \cdots s'_k$, missä $s_i, s'_i \in S$ tai $s_i^{-1}, s_i'^{-1} \in S$. Näin ollen ryhmän G Cayley graafissa solmujen g ja h välillä on kaaripolku $e_1, \ldots, e_{n+k}$, missä kaaret on määritelty seuraavasti: $\iota(e_1) = \{g, gs_n^{-1}\}$, $\ldots$, $\iota(e_n) = \{gs_n^{-1} \cdots s_2^{-1},\ gs_n^{-1} \cdots s_1^{-1} = 1_G\}$, $\iota(e_{n+1}) = \{1_G, s'_1\}$ ja $\iota(e_{n+k}) = \{s'_1 \cdots s'_{k-1},\ s'_1 \cdots s'_{k-1}s'_k = h\}$.

Näin ollen ryhmän G Cayley graafi joukon S suhteen on yhtenäinen. □

Seuraavaksi määritellään ryhmälle G metriikka sen Cayley graafin avulla. Olkoon G ryhmä, S sen virittäjäjoukko ja muodostetaan ryhmän G Cayley graafi virittäjäjoukon S suhteen. Määritellään, että jokaisen graafin Cayley(G, S) kaaren pituus on

1. Asetetaan nyt alkioiden $g, h \in G$ väliseksi etäisyydeksi lyhimmän solmujen g ja h välisen kaaripolun pituus. Alkioiden g ja h välistä etäisyyttä merkitään $\mathrm{dist}_S(g, h)$. Jos $e_1, \ldots, e_n$ on solmujen g ja h välinen lyhin kaaripolku, niin $\mathrm{dist}_S(g, h) = n$, sillä jokaisen Cayley graafin kaaren pituus on 1. Tällä säännöllä voidaan määrittää metriikka ryhmään G:

Määritelmä 4.7 (Sanametriikka)**.** Olkoon G ryhmä ja S sen virittäjäjoukko. Olkoon $\mathrm{dist}_S : G \times G \to \mathbb{N}$, $\mathrm{dist}_S(g, h) = n$, kun n on lyhimmän solmujen g ja h välisen kaaripolun pituus graafissa $\mathrm{Cayley}(G, S)$. Kuvaus dist_S on ryhmän G metriikka, jota kutsutaa *sanametriikaksi joukon S suhteen.*

Lemma 4.8. Funktio dist_S on metriikka ryhmässä G.

Todistus. Oletetaan, että G on ryhmä, S sen virittäjäjoukko ja $\mathrm{Cayley}(G, S)$ ryhmän G Cayley graafi.

Oletetaan, että $g, h \in G$ ja $\mathrm{dist}_S(g, h) = n$. On olemassa jokin lyhin kaaripolku $e_1, \ldots, e_n$ solmujen g ja h välillä. Nyt $\iota(e_1) = \{g, gs_1^{\varepsilon_1}\}$ jollain $s \in S$ ja $\varepsilon_1 = \pm 1$. Vastaavasti $\iota(e_i) = \{gs_1^{\varepsilon_1} \cdots s_{i-1}^{\varepsilon_{i-1}},\ gs_1^{\varepsilon_1} \cdots s_i^{\varepsilon_i}\}$, missä $s_j \in S$ ja $\varepsilon_j = \pm 1$ jokaisella $1 \leq j \leq n$. Tällöin $\iota(e_n) = \{gs_1^{\varepsilon_1} \cdots s_{n-1}^{\varepsilon_{n-1}},\ gs_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} = h\}$.

Solmujen h ja g välillä on kaaripolku $\bar{e_1}, \ldots, \bar{e_n}$, missä $\bar{e_i} = e_{n+1-i}$. Tällöin $\iota(\bar{e_1}) = \{h, gs_1^{\varepsilon_1} \cdots s_{n-1}^{\varepsilon_{n-1}}\}, \ldots,\ \iota(\bar{e_n}) = \{gs_1^{\varepsilon_1}, g\}$. Näin ollen $\mathrm{dist}_S(h, g) = n$, sillä jokin kaaripolkua $\bar{e_1}, \ldots, \bar{e_n}$ lyhyempi kaaripolku solmujen h ja g välillä graafissa $\mathrm{Cayley}(G, S)$ olisi ristiriidassa oletuksen $\mathrm{dist}_S(g, h) = n$ kanssa.

Lisäksi selvästi pätee $\mathrm{dist}_S(g, h) = 0$, jos ja vain jos $g = h$, sillä jokaisesta solmusta lyhin polku takaisin itseensä on nollan pituinen, ja toisaalta jokainen muu solmu kuin g itse on vähintään etäisyydellä yksi solmusta g.

Oletetaan, että on olemassa jotkin $g, h, g' \in G$, joille ei päde kolmioepäyhtälö, eli $\mathrm{dist}_S(g, h) > \mathrm{dist}_S(g, g') + \mathrm{dist}_S(g', h)$. Oletetaan, että $\mathrm{dist}_S(g, h) = n$, $\mathrm{dist}_S(g, g') = m$ ja $\mathrm{dist}_S(g', h) = l$. Tällöin $e_1, \ldots, e_n$ on kaaripolku solmujen g ja h välillä, $\bar{e_1}, \ldots, \bar{e_m}$ on on kaaripolku solmujen g ja g' välillä ja $\tilde{e_1}, \ldots, \tilde{e_l}$ on kaaripolku solmujen g' ja h välillä. Tällöin $\bar{e_1}, \ldots, \bar{e_m}, \tilde{e_1}, \ldots, \tilde{e_l}$ on kaaripolku solmujen g ja h välillä, ja vastaoletuksen nojalla $m + l < n$. Tällöin $\mathrm{dist}_S(g, h) \neq n$, mikä on ristiriidassa alkuperäisen oletuksen kanssa. $\square$

Lemma 4.9. Ryhmän G sanametriikka virittäjäjoukon S suhteen on vaseninvariantti, eli $\mathrm{dist}_S(g, g') = \mathrm{dist}_S(hg, hg')$ jokaisella $h, g, g' \in G$.

Todistus. Oletetaan, että $h, g, g' \in G$ ja $\mathrm{dist}_S(g, g') = n$. Määritelmän nojalla ryhmän G Cayley graafissa lyhin solmujen g ja g' välinen kaaripolku on muotoa $e_1, \ldots, e_n$, missä kaaren e_i päätepisteet ovat $gs_1 \cdots s_{i-1}$ ja $gs_1 \cdots s_i$, ja $s_i \in S$ tai $s_i^{-1} \in S$. Näin ollen $g' = gs_1 \cdots s_n$ ja solmujen hg ja hg' välillä on kaaripolku $\bar{e}_1, \cdots, \bar{e}_n$, missä kaaren $\bar{e}_i$ päätepisteet ovat $hgs_1 \cdots hgs_{i-1}$ ja $hgs_1 \cdots s_i$. Tämä kaaripolku on myös lyhin solmujen hg ja hg' välinen kaaripolku, sillä muuten $e_1, \ldots, e_n$ ei olisi lyhin solmujen g ja g' välinen kaaripolku. Näin ollen $\mathrm{dist}_S(hg, hg') = n$. $\square$

Määritelmä 4.10 (Sananormi)**.** Olkoon G ryhmä ja S sen äärellinen virittäjäjoukko. Alkion $g \in G$ *sananormiksi* kutsutaan alkion g pituutta aakkoston $S \cup S^{-1}$ sanana ja merkitään $|g|_S$.

Huomautus. Olkoon G ryhmä ja S sen äärellinen virittäjäjoukko. Ryhmän G alkiolla g on jokin lyhin esitys virittäjien $S \cup S^{-1}$ suhteen, eli ryhmässä G pätee $g = s_1 \cdots s_n$ joillain $s_i \in S \cup S^{-1}$. Nyt aakkoston $S \cup S^{-1}$ sanana $s_1 \cdots s_n$ on lyhin sellainen sana, jolle $\pi_S(s_1 \cdots s_n) = g$. Tällöin alkion g pituus aakkoston $S \cup S^{-1}$ sanana on n, eli toisin sanoen $|g|_S = n$.

Toisaalta ryhmän G Cayley graafissa $\mathrm{Cayley}(G, S)$ lyhin kaaripolku solmun 1 ja solmun g välillä on $e_1, \ldots, e_n$, missä $\iota(e_i) = \{s_1 \cdots s_{i-1}, s_1 \cdots s_i\}$, eli $\mathrm{dist}_S(1, g) = n$. Näin ollen $\mathrm{dist}_S(1, g) = |g|_S$.

Huomautus. Lemman 4.9 nojalla jokaisella $g, h \in G$ pätee

$$\mathrm{dist}_S(g, h) = \mathrm{dist}_S(g^{-1}g, g^{-1}h) = \mathrm{dist}_S(1, g^{-1}h) = |g^{-1}h|_S.$$

Sanametriikan määrittely ei ole yksikäsitteistä: ryhmän eri virittäjäjoukot määräävät ryhmälle eri näköiset Cayley graafit, jotka eivät välttämättä ole isometrisiä keskenään. Ryhmälle voidaan siis määritellä eri sanametriikoita. Seuraavassa lauseessa kuitenkin todistetaan, että eri virittäjäjoukkojen suhteen muodostetut metriikat ovat keskenään bilipschitz ekvivalentit.

Lause 4.11. Olkoon G äärellisesti viritetty ryhmä. Jos S ja $\bar{S}$ ovat ryhmän G äärellisiä virittäjäjoukkoja, niin sanametriikat dist_S ja $\mathrm{dist}_{\bar{S}}$ ovat bilipschitz ekvivalentit.

Todistus. Halutaan osoittaa, että on olemassa sellainen vakio $L > 0$, että kaikilla $g, g' \in G$ pätee

$$\frac{1}{L} \mathrm{dist}_S(g, g') \leq \mathrm{dist}_{\bar{S}}(g, g') \leq L \, \mathrm{dist}_S(g, g').$$

Oletetaan, että $\bar{s} \in \bar{S}$. Alkio $\bar{s}$ voidaan ilmaista joukon S virittäjien avulla. Määritellään $a = \max\{\mathrm{dist}_S(\bar{s}, 1_G) \mid \bar{s} \in \bar{S}\}$. Vastaavasti määritellään $b = \max\{\mathrm{dist}_{\bar{S}}(s, 1_G) \mid s \in S\}$. Valitaan lopuksi $L = \max\{a, b\}$.

Oletetaan, että $g \in G$. Alkio g voidaan ilmaista virittäjien avulla sievennetyssä muodossa $s_1 \cdots s_n$, missä $s_i \in S \cup S^{-1}$. Tällöin $\mathrm{dist}_S(g, 1_G) = n$ ja

$$\mathrm{dist}_{\bar{S}}(g, 1_G) = |s_1 \cdots s_n|_{\bar{S}} \leq bn \leq L\,\mathrm{dist}_S(g, 1_G),$$

sillä sanan $g = s_1 \cdots s_n$ pituus aakkoston $\bar{S} \cup \bar{S}^{-1}$ sanana on korkeintaan $nb = n \cdot \max\{\mathrm{dist}_{\bar{S}}(s, 1_G) \mid s \in S\}$.

Vastaavasti pääteltäessä saadaan, että

$$\mathrm{dist}_S(g, 1_G) \leq ak \leq L\,\mathrm{dist}_{\bar{S}}(g, 1_G),$$

kun $\mathrm{dist}_{\bar{S}}(g, 1_G) = k$. Yhdistämällä nämä päätelmät saadaan, että kaikille $g \in G$ pätee epäyhtälö

$$\frac{1}{L}\,\mathrm{dist}_S(g, 1_G) \leq \mathrm{dist}_{\bar{S}}(g, 1_G) \leq L\,\mathrm{dist}_S(g, 1_G).$$

Vastaavanlaisella päättelyllä saadaan myös, että kaikilla $g \in G$ pätee

$$\frac{1}{L}\,\mathrm{dist}_S(1_G, g) \leq \mathrm{dist}_{\bar{S}}(1_G, g) \leq L\,\mathrm{dist}_S(1_G, g).$$

Oletetaan sitten, että $g, g' \in G$. Jokainen ryhmä toimii itseensä transitiivisesti, eli $g' = hg$ jollain $h \in G$. Koska sanametriikat ovat vaseninvariantteja, niin

$$\begin{aligned}
\mathrm{dist}_S(g, g') &= \mathrm{dist}_S(hh^{-1}g, hg) = \mathrm{dist}_S(h^{-1}g, g) = |(h^{-1}g)^{-1}g|_S \\
&= |(h^{-1}g)g^{-1}|_S = \mathrm{dist}_S(h, 1_G).
\end{aligned}$$

ja

$$\mathrm{dist}_{\bar{S}}(g, g') = \mathrm{dist}_{\bar{S}}(h, 1_G).$$

Näin ollen kaikilla $g, g' \in G$

$$\frac{1}{L}\,\mathrm{dist}_S(g, g') \leq \mathrm{dist}_{\bar{S}}(g, g') \leq L\,\mathrm{dist}_S(g, g').$$

$\square$

Tärkeä lauseen 4.11 seuraus on, että jos G on ryhmä, jolla on virittäjäjoukot S ja $\bar{S}$, niin metrisinä avaruuksina avaruudet (G, dist_S) ja $(G, \mathrm{dist}_{\bar{S}})$ ovat kvasi-isometriset.

Toisinaan graafeihin liitetään *geometrinen toteutus*, jota voidaan havainnollistaa samanlaisilla kuvilla kuin kuvat 4.1 ja 4.2. Geometrisessa toteutuksessa graafin kaaret voidaan ajatella janoiksi, jotka liittävät solmut toisiinsa. Tällöin graafeihin voidaan määritellä *graafien standardi metriikka*. Ryhmän G Cayley graafit eri virittäjäjoukkojen suhteen tällä standardilla metriikalla varustettuna ovat keskenään kvasi-isometriset, eli "tarpeeksi kaukaa katsottaessa ne näyttävät samoilta." Ryhmälle G määritellään sitten sanametriikka sen Cayley graafin metriikasta rajoittamalla metriikka graafin solmuihin eli ryhmän G alkioihin ([2], s.228-229).

4.2.2 Ryhmien kasvu

Tässä alaluvussa tarkastellaan, mitä ryhmien kasvu tarkoittaa. Erityisesti todistetaan, että ryhmän kasvu ei riipu valitusta virittäjäjoukosta eikä kantapisteestä. Eri virittäjien suhteen tarkasteltavat kasvufunktiot ovat asymptoottisesti ekvivalentit, eli ne kuuluvat samaan kasvun ekvivalenssiluokkaan.

Funktioiden kasvusta

Jotta voidaan tarkastella ryhmien kasvua, määritellään relaatiot $\preceq$ ja $\asymp$ funktioille. Niiden avulla voidaan vertailla funktioiden kasvua toisiinsa nähden.

Määritelmä 4.12 (Funktioiden asymptoottinen vertailu)**.** Oletetaan, että $X \subset \mathbb{R}$, ja $f, g : X \to \mathbb{R}$. Oletetaan, että on olemassa sellaiset $a, b > 0$ ja $x_0 \in \mathbb{R}$, että kaikilla $x \in X$, joille pätee $x \geq x_0$, pätee myös $bx \in X$ ja

$$f(x) \leq ag(bx).$$

Tällöin merkitään $f \preceq g$. Jos $f \preceq g$ ja $g \preceq f$, niin f ja g ovat *asymptoottisesti ekvivalentit*. Tätä merkitään $f \asymp g$.

Lause 4.13. Olkoon $X \subset \mathbb{R}$. Relaatio $\asymp$ on ekvivalenssirelaatio kuvausten $X \to \mathbb{R}$ joukossa.

Todistus. Olkoon $X \subset \mathbb{R}$ ja $f, g, h : X \to \mathbb{R}$. Olkoon $x_0 = \min_{x' \in X} x'$. Tällöin kaikilla $x \in X$, joilla $x \geq x_0$ pätee, että ensinnäkin $x \in X$ ja lisäksi $f(x) \leq 1 \cdot f(1 \cdot x)$, joten

$f \preceq f$. Tällöin $f \asymp f$, eli relaatio $\asymp$ on refleksiivinen kuvausten $X \to \mathbb{R}$ joukossa. Oletetaan sitten, että $f \asymp g$. Määritelmän nojalla tällöin $f \preceq g$ ja $g \preceq f$, joten myös $g \asymp f$. Näin ollen relaatio $\asymp$ on refleksiivinen kuvausten $X \to \mathbb{R}$ joukossa.

Jäljellä on enää relaation $\asymp$ transitiivisuuden osoittaminen. Oletetaan, että $f \asymp g$ ja $g \asymp h$. Tällöin erityisesti $f \preceq g$, joten on olemassa sellaiset vakiot $a, b > 0$ ja $x_0 \in \mathbb{R}$, että kaikilla $x \in X$, $x \geq x_0$, pätee $bx \in X$ ja $f(x) \leq ag(bx)$. Vastaavasti $g \preceq h$, mistä seuraa, että on olemassa sellaiset vakiot $c, d > 0$ ja piste $y_0 \in \mathbb{R}$, että kaikilla $y \in X$, $y \geq y_0$, pätee $dy \in X$ ja $g(y) \leq ch(dy)$.

Merkitään $z = \max\{x_0, \frac{y_0}{b}\}$. Nyt $ac, db > 0$ ja jos $x \in X$, $x \geq z$ saadaan, että $bx \geq b\frac{y_0}{b} = y_0$, joten $dbx \in X$. Tällöin

$$f(x) \leq ag(bx) \leq ach(dbx),$$

joten $f \preceq h$. Vastaavasti käyttämällä oletuksia $h \preceq g$ ja $g \preceq f$ voidaan päätellä, että $h \preceq f$. Määritelmän nojalla $f \asymp h$, joten $\asymp$ on transitiivinen relaatio kuvausten $X \to \mathbb{R}$ joukossa. □

Määritelmä 4.14 (Kasvun ekvivalenssiluokka)**.** Ekvivalenssiluokkia ekvivalenssirelaation $\asymp$ suhteen kutsutaan *kasvun ekvivalenssiluokiksi.*

Olkoon $X \subset \mathbb{R}$ ja $f : X \to \mathbb{R}$. Funktion f kanssa samaan ekvivalenssiluokkaan kuuluvat kaikki kuvaukset $g : X \to \mathbb{R}$, joilla $f \asymp g$.

Määritelmä 4.15 (Tasaisesti diskreetti metrinen avaruus)**.** Metrinen avaruus X on *tasaisesti diskreetti*, jos on olemassa sellainen kuvaus $\phi : \mathbb{R}_+ \to \mathbb{N}$, että jokainen r-säteinen suljettu kuula $\bar{B}(x, r) \subset X$ sisältää korkeintaan $\phi(r)$ alkiota. Tasaisesti diskreetissä avaruudessa siis jokaisen r-säteisen suljetun kuulan mahtavuudella on jokin säteestä r riippuva yläraja.

Erityisesti äärellisesti viritetyt ryhmät ovat tasaisesti diskreettejä metrisiä avaruuksia.

Lause 4.16. Jos $f : X \to Y$ on karkea Lipschitz kuvaus tasaisesti diskreettien metristen avaruuksien X ja Y välillä, niin f on Lipschitz.

Todistus. Oletetaan, että (X, d_X) ja (Y, d_Y) ovat tasaisesti diskreettejä metrisiä avaruuksia. Tällöin jokaisella pisteparilla $x, x' \in X$, $x \neq x'$, pätee $d_X(x, x') \geq \varepsilon$, jollain

$\varepsilon > 0$, eli kaikki pisteet ovat vähintään etäisyyden ε päässä toisistaan. Erityisesti saadaan, että $\varepsilon^{-1} d_X(x, x') \geq 1$.

Olkoon $f : X \to Y$ (L, C)-karkea Lipschitz kuvaus. Tällöin kaikilla $x, x' \in X$, $x \neq x'$, pätee

$$
\begin{aligned}
d_Y(f(x), f(x')) &\leq L d_X(x, x') + C \leq L d_X(x, x') + C \left(\frac{1}{\varepsilon} d_X(x, x') \right) \\
&= \left(L + \frac{C}{\varepsilon} \right) d_X(x, x'),
\end{aligned}
$$

missä $L + \frac{C}{\varepsilon} > 0$. Siispä f on $(L + \frac{C}{\varepsilon})$-Lipschitz. □

Määritelmä 4.17 (Kasvufunktio)**.** Olkoon X diskreetti metrinen avaruus ja $x \in X$ kantapiste. Suljetun, x-keskeisen ja R-säteisen kuulan mahtavuutta kutsutaan *kasvufunktioksi*. Merkitään tätä

$$
\mathcal{B}_{X,x}(R) := \operatorname{card} \bar{B}(x, R).
$$

Seuraavaksi osoitetaan, että kasvufunktion määritelmässä ei tarvitse tarkentaa minkä avaruuden X pisteen x suhteen kasvufunktiota tarkastellaan. Tämä johtuu seuraavasta lauseesta, josta ilmenee, että *kasvun ekvivalenssiluokka on kvasi-isometria invariantti.*

Lause 4.18. Olkoot (X, x_0) ja (Y, y_0) tasaisesti diskreettejä kantapisteavaruuksia. Jos (X, x_0) ja (Y, y_0) ovat kvasi-isometrisia avaruuksia, niin $\mathcal{B}_{X,x_0} \asymp \mathcal{B}_{Y,y_0}$.

Todistus. Merkitään avaruuden X metriikkaa d_X ja avauuden Y metriikkaa d_Y. Olkoon $f \colon (X, x_0) \to (Y, y_0)$ (L', C)–kvasi-isometria, ja olkoon $\bar{f} \colon (Y, y_0) \to (X, x_0)$ sen karkea käänteiskuvaus. Lauseen 4.16 nojalla on olemassa sellaiset positiiviset vakiot L_X ja L_Y, että f on L_X–Lipschitz ja $\bar{f}$ on L_Y–Lipschitz. Merkitään $L = \max\{L_X, L_Y\}$, jolloin f ja $\bar{f}$ ovat molemmat L–Lipschitz kuvauksia.

Olkoon $R > 0$. Oletetaan, että $x \in X$ ja $d_X(x, x_0) \leq R$. Tällöin

$$
d_Y(f(x), y_0) = d_Y(f(x), f(x_0)) \leq L d_X(x, x_0) \leq LR.
$$

Siis $f\bar{B}(x_0, R) \subset \bar{B}(y_0, LR)$. Vastaavasti jos $y \in Y$ ja $d_Y(y, y_0) \leq R$, niin

$$
d_X(\bar{f}(y), x_0) = d_X(\bar{f}(y), \bar{f}(y_0)) \leq L d_Y(y, y_0) \leq LR,
$$

joten $\bar{f}\bar{B}(y_0, R) \subset \bar{B}(x_0, LR)$.

Toisaalta, jos $f(x) = f(x')$ joillain $x, x' \in X$, niin

$$d_X(x, x') \leq d_X(x, \bar{f} \circ f(x)) + d_X(\bar{f} \circ f(x'), x') \leq C + C = 2C.$$

Vastaavasti, jos $y, y' \in Y$ ja $\bar{f}(y) = \bar{f}(y')$, niin $d_Y(y, y') \leq 2C$.

Avaruudet X ja Y ovat tasaisesti diskreettejä, joten jokaisessa $2C$-säteisessä suljetussa kuulassa on korkeintaan $m_X < \infty$ alkiota avaruudessa X ja $m_Y < \infty$ alkiota avaruudessa Y. Voidaan valita $m = \max\{m_X, m_Y\}$, jolloin m on yläräja molempien avaruuksien $2C$-säteisten suljettujen kuulien mahtavuuksille.

Näin ollen

$$\operatorname{card} \bar{B}(x_0, R) \leq m \operatorname{card} \bar{B}(y_0, LR)$$

ja

$$\operatorname{card} \bar{B}(y_0, R) \leq m \operatorname{card} \bar{B}(x_0, LR),$$

eli $\mathcal{B}_{X,x_0}(R) \preceq m\mathcal{B}_{Y,y_0}(LR)$ ja $\mathcal{B}_{Y,y_0}(R) \preceq m\mathcal{B}_{X,x_0}(LR)$. Siis $\mathcal{B}_{X,x_0} \asymp \mathcal{B}_{Y,y_0}$. □

Jokainen ryhmä G toimii itseensä transitiivisesti vasemmalta, eli kaikilla $g, g' \in G$ on olemassa $h \in G$, jolla $g' = hg$. Tällöin translaatio alkion h suhteen on isometria kantapisteavaruuksien (G, g) ja (G, g') välillä. Nimittäin kuvaukselle $L_h : (G, g) \to (G, g')$, $x \mapsto hx$, pätee $L_h(g) = hg = g'$ ja lisäksi kaikilla $x, x' \in G$

$$\operatorname{dist}_S(L_h(x), L_h(x')) = \operatorname{dist}_S(hx, hx') = \operatorname{dist}_S(x, x'),$$

eli L_h on isometria kantapisteavaruuksien (G, g) ja (G, g') välillä. Lisäksi kuvauksella L_h on käänteiskuvaus $L_{h^{-1}}$, $x \mapsto h^{-1}x$, joten erityisesti funktio L_h on bijektio. Näin ollen kanstapisteavaruudet (G, g) ja (G, g') ovat isometriset, joten lauseen 4.18 nojalla ryhmien kasvufunktioita tarkastellessa voidaan jättää kantapiste merkitsemättä. Jos G on äärellisviritteinen ryhmä, ja S sen virittäjäjoukko, usein käytetään merkintää $\mathcal{B}_S(R)$ merkinnän $\mathcal{B}_G(R)$ sijasta.

Lause 4.19. Jos S ja S' ovat kaksi äärellistä ryhmän G virittäjäjoukkoa, niin kasvufunktioille pätee $\mathcal{B}_S \asymp \mathcal{B}_{S'}$.

Todistus. Tulos seuraa lauseista 4.11 ja 4.18. □

Lause 4.20. Olkoon G äärellisesti viritetty. Jos N on ryhmän G normaali aliryhmä, niin

$$\mathcal{B}_{G/N} \preceq \mathcal{B}_G.$$

Todistus. Jos S on ryhmän G äärellinen virittäjäjoukko, olkoon $\bar{S} = \{sN \mid s \in S, s \notin N\}$ sitä vastaava ryhmän G/N virittäjäjoukko. Olkoon $\pi : G \to G/N$ tekijähomomorfismi.

Halutaan näyttää, että on olemassa sellaiset vakiot $a, b > 0$ ja $r_0 \in \mathbb{R}$, että kaikilla $r \in \mathbb{N}$, $r \geq r_0$, pätee $br \in \mathbb{N}$ ja $\mathcal{B}_{G/N}(r) \leq a\mathcal{B}_G(br)$ eli yhtäpitävästi

$$\operatorname{card} \bar{B}_{G/N}(1_{G/N}, r) \leq a \operatorname{card} \bar{B}_G(1, br).$$

Oletetaan, että $r \geq 1$. Jos $gN \in \bar{B}_{G/N}(1_{G/N}, r)$, niin $gN = s_1N \cdots s_lN = \pi(g)$, missä $1 \leq l \leq r$ ja $g = s_1 \cdots s_l \in \bar{B}_G(1, r)$. Näin ollen $\bar{B}_{\bar{S}}(1_{G/N}, r) \subset \pi(\bar{B}_S(1, r))$ ja

$$\operatorname{card} \bar{B}_{\bar{S}}(1_{G/N}, r) \leq \operatorname{card} \pi(\bar{B}_S(1, r)) \leq \operatorname{card} \bar{B}_S(1, r),$$

mikä todistaa väitteen. □

Lause 4.21. Kasvufunktio on submultiplikatiivinen, eli kaikilla $r, t \in \mathbb{R}_+$ pätee

$$\mathcal{B}_S(r + t) \leq \mathcal{B}_S(r)\mathcal{B}_S(t).$$

Todistus. Olkoon G ryhmä ja S sen virittäjäjoukko. Näytetään, että

$$\bar{B}(1, n + m) \subset \bigcup_{y \in \bar{B}(1,n)} \bar{B}(y, m)$$

kaikilla $n, m \in \mathbb{N}$. Jos $n = 0 = m$, niin väite seuraa helposti, sillä $\bar{B}(1, n + m) = \bar{B}(1, n) = \{1\}$. Tällöin nimittäin $\bar{B}(1, n + m) \subset \cup_{y \in \bar{B}(1,n)} \bar{B}(y, m) = \bar{B}(1, m)$.

Jos puolestaan $n = 0$, mutta $m \neq 0$, niin $\bar{B}(1, n + m) = \bar{B}(1, m)$, ja toisaalta $\bar{B}(1, n) = \bar{B}(1, 0)$, jolloin $\cup_{y \in \bar{B}(1,n)} \bar{B}(y, m) = \bar{B}(1, m)$.

Oletetaan sitten, että $n \neq 0 \neq m$ ja $g \in \bar{B}(1, n + m)$. Tällöin voidaan kirjoittaa $g = s_1 \ldots s_k$. Jos $0 \leq k \leq n \leq m + n$, niin

$$d_S(1, g) = |g|_S = k \leq n,$$

joten $g \in \bar{B}(1, n)$. Näin ollen $g \in \cup_{y \in \bar{B}(1,n)} \bar{B}(y, m)$.

Jos puolestaan $n \leq k \leq n + m$, niin sana g voidaan jakaa osiin $g = ys_{n+1} \ldots s_k$, missä $y = s_1 \ldots s_n$ ja $k - n \leq m$.

Tällöin $d_S(y, g) = |y^{-1}g|_S = |s_{n+1} \ldots s_k|_S = k - n$, eli $g \in \bar{B}(y, m)$ ja myös $g \in \cup_{y \in \bar{B}(1,n)} \bar{B}(y, m)$.

Näin ollen kaikilla $n, m \in \mathbb{N}$ pätee

$$\bar{B}(1, n+m) \subset \bigcup_{y \in \bar{B}(1,n)} \bar{B}(y, m).$$

Tämän tarkastelu riittää, sillä jos otetaan mielivaltainen reaaliluku $r > 0$, huomataan, että $\bar{B}(1, r) = \bar{B}(1, n)$, missä n on suurin luonnollinen luku, jolle pätee $n \leq r$.

Tästä seuraa suoraan, että

$$\operatorname{card} \bar{B}(1, r+t) \leq \operatorname{card} \bar{B}(1, r) \cdot \operatorname{card} \bar{B}(1, t)$$

kaikilla $r, t > 0$. Näin ollen

$$\mathcal{B}_S(r+t) \leq \mathcal{B}_S(r)\mathcal{B}_S(t).$$

$\square$

Määritelmä 4.22. Olkoon G äärellisviritteinen ryhmä, ja S sen virittäjäjoukko. Raja-arvoa

$$\gamma_S = \lim_{n \to \infty} \mathcal{B}_S(n)^{\frac{1}{n}}$$

kutsutaan *kasvuvakioksi*. Jos $\gamma_S > 1$, niin ryhmän G sanotaan *kasvavan eksponentiaalisesti*.

Lause 4.23. Raja-arvo γ_S on olemassa.

Todistus. Oletetaan, että $r, t \in \mathbb{R}_+$. Lauseen 4.21 nojalla kasvufunktio on submultiplikatiivinen. Tästä ja logaritmin ominaisuuksista seuraa, että

$$\ln \mathcal{B}_S(r+t) \leq \ln \mathcal{B}_S(r)\mathcal{B}_S(t) \leq \ln \mathcal{B}_S(r) + \ln \mathcal{B}_S(t),$$

eli kuvaus $\ln \mathcal{B}_S(n)$ on subadditiivinen. Feketen lemmasta [5, lause 7.6.1] seuraa, että raja-arvo

$$\lim_{n \to \infty} \frac{\ln \mathcal{B}_S(n)}{n}$$

on olemassa ja äärellinen, mistä seuraa raja-arvon

$$\gamma_S = \lim_{n \to \infty} \mathcal{B}_S(n)^{\frac{1}{n}}$$

olemassaolo ja äärellisyys. $\square$

Luku 5

Algebrallisia käsitteitä

Tässä alaluvussa esitetään tämän tutkielman kannalta oleellisia algebrallisia käsitteitä. Aluksi esitellään lyhyesti ryhmän G alkioiden kommutaattorit ja niiden ominaisuuksia sekä kommutaattorialiryhmä. Tämän lisäksi esitellään ratkeavat ryhmät, nilpotentit ryhmät ja polysykliset ryhmät.

5.1 Kommutaattorit ja kommutaattorialiryhmä

Määritelmä 5.1 (Kommutaattorialiryhmä)**.** Olkoon G ryhmä ja $x, y \in G$. Alkioiden x ja y *kommutaattori* on $[x, y] = xyx^{-1}y^{-1}$. Ryhmän G *kommutaattorialiryhmä* on ryhmän G kommutaattorien virittämä aliryhmä. Sille käytetään merkintää G'. Jos $H, K \subset G$, niin merkinnällä $[H, K]$ tarkoitetaan ryhmän G aliryhmää, jonka virittäjät ovat kaikki kommutaattorit $[h, k]$, missä $h \in H$ ja $k \in K$. Näin ollen $G' = [G, G]$.

Kommutaattoreille pätevät seuraavat ominaisuudet, jotka ovat hyödyllisiä tarkastellessa kommutaattorialiryhmiä.

Lause 5.2. Olkoon $(G, \cdot)$ ryhmä ja $x, y, z \in G$. Tällöin seuraavat ominaisuudet pätevät:

(1) $[x, y]^{-1} = [y, x]$

(2) $[x^{-1}, y] = [x^{-1}, [y, x]][y, x]$

(3) $[x, yz] = [x, y][y, [x, z]][x, z]$

(4) $[xy, z] = [x, [y, z]][y, z][x, z]$

(5) $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.

Lemma 5.3. Ryhmä G on vaihdannainen, jos ja vain jos sen kommutaattorialiryhmä on triviaali eli $G' = \{1_G\}$. Lisäksi pätee, että kommutaattorialiryhmä G' on ryhmän G karakteristinen aliryhmä ja siten normaali.

Todistus. Lemman ensimmäinen osa seuraa hyvin suoraviivaisesti määritelmistä. Jos G on vaihdannainen, niin kaikilla $x, y \in G$ pätee $xy = yx$, eli $xyx^{-1}y^{-1} = 1_G$. Näin ollen kommutaattorialiryhmä $G' = \{1_G\}$. Toisaalta jos $G' = \{1_G\}$, niin $xy = yx$ kaikilla $x, y \in G$, ja täten G on vaihdannainen.

Näytetään sitten, että kaikilla ryhmän G automorfismeilla ϕ, pätee $G' = \phi(G')$. Merkitään $S = \{[x, y] \mid x, y \in G\}$. Tällöin S on kommutaattorialiryhmän G' virittäjäjoukko ja sille pätee $S = \phi(S)$. Jos nimittäin $[x, y] \in S$ ja $\phi([x, y]) \in \phi(S)$, niin $\phi([x, y]) = [\phi(x), \phi(y)] \in S$. Siis $\phi(S) \subset S$. Toisaalta on olemassa yksikäsitteiset $g, h \in G$, joille pätee $\phi(g) = x$ ja $\phi(h) = y$. Tällöin

$$[x, y] = xyx^{-1}y^{-1} = \phi(g)\phi(h)\phi(g)^{-1}\phi(h)^{-1} = \phi([g, h]),$$

missä $[g, h] \in S$. Siis $S \subset \phi(S)$.

Näin ollen myös $G' = \phi(G')$ eli ryhmän G kommutaattorialiryhmä G' on ryhmän G karakteristinen aliryhmä. Lauseen 2.14 nojalla karakteristiset aliryhmät ovat normaaleja, joten kommutaattorialiryhmä G' on ryhmän G normaali aliryhmä. □

Määritelmä 5.4 (Ryhmän abelianisaatio)**.** Ryhmän G tekijäryhmää kommutaattorialiryhmän G' suhteen merkitään $G_{ab} = G/G'$ ja kutsutaan ryhmän G *abelianisaatioksi*, ja tekijäkuvausta $p : G \to G_{ab}$ kutsutaan *abelianisaatio homomorfismiksi.*

Lemma 5.5. Ryhmän G abelianisaatio G_{ab} on vaihdannainen ryhmä. Lisäksi pätee, että jokainen homomorfismi $\varphi : G \to A$, missä A on vaihdannainen ryhmä, voidaan hajottaa kulkemaan tekijäryhmän G_{ab} kautta: on olemassa sellainen homomorfismi $\bar{\varphi} : G_{ab} \to A$, että $\varphi = \bar{\varphi} \circ p$, missä $p : G \to G_{ab}$ on tekijäkuvaus. Siis alla oleva kaavio kommutoi:

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "p"] & A \\ G_{ab} \arrow[ur, "\bar{\varphi}"] & \end{tikzcd}$$

Todistus. Osoitetaan ensiksi, että abelianisaatio on vaihdannainen ryhmä. Lemman 5.3 nojalla G' on ryhmän G normaali aliryhmä. Tällöin abelianisaatio G_{ab} on ryhmä.

Jälleen lemman 5.3 nojalla vaihdannaisuuden osoittamiseen riittää näyttää, että $(G_{ab})' = \{G'\} = 1_{G_{ab}}$. Alkiot $[gG', hG']$, missä $g, h \in G$, virittävät ryhmän G'_{ab}. Tekijäryhmän laskusäännöistä seuraa, että

$$[gG', hG'] = ghg^{-1}h^{-1}G' = G',$$

sillä $ghg^{-1}h^{-1} \in G'$. Tästä seuraa, että $G'_{ab} = \{G'\}$, mikä todistaa vaihdannaisuuden.

Olkoon A vaihdannainen ryhmä ja $\varphi : G \to A$ homomorfismi. Osoitetaan nyt, että $G' \subset \ker \varphi$. Olkoon $x, y \in G$, jolloin $[x, y]$ on eräs aliryhmän G' virittäjä. Ryhmän A vaihdannaisuudesta seuraa, että

$$\varphi([x, y]) = \varphi(x)\varphi(x)^{-1}\varphi(y)\varphi(y)^{-1} = 1_A,$$

eli $[x, y] \in \ker \varphi$. Tästä seuraa, että $G' \subset \ker \varphi$. Lemman 2.5 nojalla φ voidaan hajottaa kulkemaan tekijäryhmän $G_{ab} = G/G'$ kautta, eli on olemassa yksikäsitteinen homomorfismi $\bar{\varphi} : G_{ab} \to A$, jolle pätee $\bar{\varphi} \circ p = \varphi$. $\square$

Ryhmän G abelianisaation voi ajatella vaihdannaisena versiona ryhmästä G. Se on ryhmä, jossa kaikilla ryhmän G alkioilla näyttäisi pätevän yhtälö $xy = yx$. Oletetaan, että G on ryhmä ja $x, y \in G$. Koska jokainen kommutaattori $[x^{-1}, y^{-1}] = x^{-1}y^{-1}xy \in G'$, niin tekijäryhmässä G_{ab} sivuluokille pätee yhtälö $xyG' = yxG'$. Näin ollen ryhmän G abelianisaatio on ryhmä, jossa yhtälö $[xy] = [yx]$ pätee kaikilla alkioilla $x, y \in G$.

5.2 Ratkeavat ryhmät

Seuraavaksi esitellään ratkeavat ryhmät. Ratkeavat ryhmät ovat sellaisia ryhmiä, joilla on äärellisen pituinen kommutaattorialiryhmien jono. Kommutaattorialiryhmien jono muodostetaan ottamalla ryhmästä sen kommutaattorialiryhmä, ja sen jälkeen jonon jäsenet saadaan iteratiivisesti ottamalla edellisen jäsenen kommutaattorialiryhmä. Tässä luvussa osoitetaan yleisesti ratkeavien ryhmien tuloksia, mutta tutkielman viimeisessä luvussa ollaan kiinnostuneita vain äärellisesti viritetyistä ratkeavista ryhmistä.

Määritelmä 5.6 (Kommutaattorialiryhmien jono)**.** Olkoon G ryhmä. Määritellään sen *korkeamman asteen kommutaattorialiryhmät* induktiivisesti

$$G^{(0)} = G, G^{(1)} = G', \dots, G^{(k+1)} = \left(G^{(k)}\right)', \dots.$$

Näistä voidaan muodostaa ryhmälle G subnormaali laskeva jono

$$G \trianglerighteq G' \trianglerighteq \cdots \trianglerighteq G^{(k)} \trianglerighteq G^{(k+1)} \trianglerighteq \dots,$$

jota kutsutaan *kommutaattorialiryhmien jonoksi.*

Lause 5.7. Aliryhmä $G^{(k)}$ on ryhmän G karakteristinen aliryhmä jokaisella $k \in \mathbb{N}$.

Todistus. Lauseen 5.3 nojalla $G^{(k+1)}$ on ryhmän $G^{(k)}$ karakteristinen aliryhmä jokaisella $k \geq 0$. Lauseen 2.15 nojalla tästä seuraa, että $G^{(k)}$ on ryhmän G karakteristinen aliryhmä jokaisella k.

Vaihtoehtoisesti väite voidaan todistaa induktiolla. Lauseen 5.3 nojalla kommutaattorialiryhmä G' on ryhmän G karakteristinen aliryhmä. Oletetaan sitten, että jokaisella $k \leq n$ pätee, että $G^{(k)}$ on ryhmän G karakteristinen aliryhmä, ja osoitetaan, että tällöin myös $G^{(n+1)}$ on ryhmän G karakteristinen aliryhmä.

Olkoon $\varphi : G \to G$ ryhmän G automorfismi ja merkitään $S = \{[x, y] \mid x, y \in G^{(n)}\}$. Joukko S on siis ryhmän $G^{(n+1)}$ virittäjäjoukko. Oletetaan, että $[x, y] \in S$. Tällöin induktio-oletuksen nojalla $\varphi([x, y]) = [\varphi(x), \varphi(y)]$, missä $\varphi(x), \varphi(y) \in G^{(n)}$. Näin ollen $\varphi([x, y]) \in S$ eli $\varphi(S) \subset S$.

Induktio-oletuksen nojalla $G^{(n)} = \varphi(G^{(n)})$, joten on olemassa sellaiset alkiot $x', y' \in G^{(n)}$, että $x = \varphi(x')$ ja $y = \varphi(y')$. Tällöin $[x, y] = \varphi(x')\varphi(y')\varphi(x')^{-1}\varphi(y')^{-1} = \varphi([x', y'])$, missä $[x', y'] \in S$. Siispä $S \subset \varphi(S)$.

Koska S on ryhmän $G^{(n+1)}$ virittäjäjoukko ja $S = \varphi(S)$, niin $G^{(n+1)} = \varphi(G^{(n+1)})$. Näin ollen $G^{(n+1)}$ on ryhmän G karakteristinen aliryhmä. □

Määritelmä 5.8 (Ratkeavat ryhmät)**.** Jos on olemassa sellainen $k \in \mathbb{N}$, että $G^{(k)} = \{1_G\}$, niin sanotaan, että ryhmä G on ratkeava.

Lause 5.9. Olkoon G ratkeava ja H ryhmän G aliryhmä. Tällöin myös H on ratkeava.

Todistus. Oletetaan, että G on ratkeava. On siis olemassa jokin luonnollinen luku k, jolla $G^{(k)} = \{1_G\}$. Osoitetaan induktiolla, että $H^{(i)} \leqslant G^{(i)}$ jokaisella $i \geq 1$. Jos

$[x, y] \in H'$ virittäjäalkio, niin $x, y \in H \subset G$, joten $[x, y]$ on määritelmän nojalla myös ryhmän G' virittäjäalkio. Näin ollen $H^{(1)} \leqslant G^{(1)}$.

Oletetaan sitten, että jokaisella $i \leq n$ pätee, että $H^{(i)} \leqslant G^{(i)}$. Olkoon $[x, y] \in H^{(n+1)}$ virittäjäalkio. Määritelmän nojalla $x, y \in H^{(n)}$, ja induktio-oletuksen nojalla $H^{(n)} \leqslant G^{(n)}$, joten $[x, y]$ on myös ryhmän $G^{(n+1)}$ virittäjäalkio. Näin ollen $H^{(n+1)} \leqslant G^{(n+1)}$.

Tästä seuraa erityisesti, että $H^{(k)} \leqslant G^{(k)} = \{1_G\}$, joten H on ratkeava. □

Todistetaan seuraavaksi aputulos, jota hyödynnetään lauseiden 5.11 ja 5.12 todistuksissa.

Lemma 5.10. Olkoon G ryhmä, N sen normaali aliryhmä ja $\pi : G \to G/N$ tekijähomomorfismi. Tällöin jokaisella $k \in \mathbb{N}$ pätee $\pi(G^{(k)}) = (G/N)^{(k)}$.

Todistus. Osoitetaan induktiolla, että jokaisella $k \in \mathbb{N}$ pätee $\pi(G^{(k)}) = (G/N)^{(k)}$. Alkuaskeleessa oletetaan, että $k = 0$, jolloin väite pätee, sillä $\pi(G^{(0)}) = \pi(G) = G/N = (G/N)^{(0)}$.

Oletetaan sitten, että jokaisella $k \leq n$ pätee $\pi(G^{(k)}) = (G/N)^{(k)}$. Osoitetaan, että tällöin $\pi(G^{(n+1)}) = (G/N)^{(n+1)}$. Tarkastellaan ryhmän $G^{(n+1)}$ virittäjää $[x, y]$, missä $x, y \in G^{(n)}$. Induktio-oletuksen nojalla $\pi(x), \pi(y) \in (G/N)^{(n)}$, joten kommutaattorin $[x, y]$ kuva $\pi(x)\pi(y)\pi(x)^{-1}\pi(y)^{-1}$ on määritelmän nojalla ryhmän $(G/N)^{(n+1)}$ virittäjä. Näin ollen $\pi(G^{(n+1)}) \subset (G/N)^{(n+1)}$.

Olkoon sitten $[X, Y] \in (G/N)^{(n+1)}$ virittäjä. Määritelmän nojalla alkiot $X, Y \in (G/N)^{(n)}$, joten induktio-oletuksesta seuraa, että $X = \pi(x')$ ja $Y = \pi(y')$ joillain $x', y' \in G^{(n)}$. Näin ollen

$$[X, Y] = \pi(x')\pi(y')\pi(x')^{-1}\pi(y')^{-1} = \pi(x'y'x'^{-1}y'^{-1}),$$

missä $x'y'x'^{-1}y'^{-1}$ on ryhmän $G^{(n+1)}$ virittäjä. Näin ollen $(G/N)^{(n+1)} \subset \pi(G^{(n+1)})$.

Näin ollen $\pi(G^{(k)}) = (G/N)^{(k)}$ jokaisella $k \in \mathbb{N}$. □

Lemmasta 5.10 seuraa suoraan, että jokaisen ratkeavan ryhmän tekijäryhmä normaalin aliryhmän suhteen on ratkeava.

Lause 5.11. Olkoon G ryhmä ja N sen normaali aliryhmä. Jos G on ratkeava, niin G/N on ratkeava.

Todistus. Olkoon $\pi : G \to G/N$ tekijähomomorfismi. Jos ryhmä G on ratkeava, on olemassa jokin sellainen luku $k \in \mathbb{N}$, että $G^{(k)} = \{1_G\}$. Tällöin lemman 5.10 nojalla $(G/N)^{(k)} = \pi(G^{(k)}) = \{1_{G/N}\}$ eli tekijäryhmä G/N on ratkeava. □

Lause 5.12. Olkoon G ryhmä ja N sen normaali aliryhmä. Jos ryhmät N ja G/N ovat ratkeavia, niin myös G on ratkeava.

Todistus. Aliryhmä N oletetaan ratkeavaksi, joten on olemassa sellainen $k \in \mathbb{N}$, että $N^{(k)} = \{1_G\}$. Vastaavasti on olemassa jokin $k' \in \mathbb{N}$, jolla $(G/N)^{(k')} = \{1_{G/N}\}$.

Olkoon jälleen $\pi : G \to G/N$ tekijähomomorfismi. Lemman 5.10 nojalla jokaisella $i \in \mathbb{N}$ pätee $\pi(G^{(i)}) = (G/N)^{(i)}$. Erityisesti tästä voidaan päätellä, että $\pi(G^{(k')}) = (G/N)^{(k')} = \{1_{G/N}\}$. Näin ollen jos $g \in G^{(k')}$, niin $gN = N$, eli $g \in N$. Siispä $G^{(k')}$ on ryhmän N aliryhmä. Tästä voidaan induktiolla johtaa, että $G^{(k'+i)} \leqslant N^{(i)}$ jokaisella $i \in \mathbb{N}$. Alkutapaus $i = 0$ on jo osoitettu.

Oletetaan, että $G^{(k'+i)}$ on ryhmän $N^{(i)}$ aliryhmä jollain $i \geq 0$ ja $[x, y] \in G^{(k'+i+1)}$. Tällöin $x, y \in G^{(k'+i)}$, joten oletuksen nojalla $x, y \in N^{(i)}$. Tästä seuraa, että $[x, y]$ on ryhmän $N^{(i+1)}$ virittäjä. Näin ollen $G^{(k'+i+1)} \leqslant N^{(i+1)}$.

Erityisesti tästä seuraa, että $G^{(k'+k)} \leqslant N^{(k)} = \{1_G\}$ eli G on ratkeava. □

Jokainen vaihdannainen ryhmä on ratkeava, sillä vaihdannaisella ryhmällä G on jono muotoa

$$G \trianglerighteq G' = \{1_G\}.$$

Eräs esimerkki ratkeavasta ryhmästä, joka ei ole vaihdannainen, on symmetrinen ryhmä $S_3 = \{(1), (12), (23), (13), (123), (132)\}$. Tutkimalla mahdollisia kommutaattoreja $[x, y]$, missä $x, y \in S_3$, saadaan alkiot $(1), (123)$ ja (132). Näin ollen symmetrisen ryhmän S_3 kommutaattorialiryhmän virittäjät ovat alkiot $(1), (123)$ ja (132). Koska $(123)^2 = (132)$, $(123)^3 = (1)$, $(132)^2 = (123)$ ja $(132) = (123)^{-1}$, niin $S_3' = \{(1), (123), (132)\}$. Tätä aliryhmää kutsutaan *alternoivaksi ryhmäksi*, ja merkitään A_3. Nyt puolestaan kaikilla $x', y' \in S_3'$ pätee $[x', y'] = (1)$, eli $(S_3)^{(2)} = \{(1)\}$. Näin ollen symmetrinen ryhmä S_3 on ratkeava.

Esimerkissä 5.17 osoitetaan, että diskreetti Heisenbergin ryhmä $H_3(\mathbb{Z})$ on ratkeava.

Huomautus. Joissain lähteissä ratkeavat ryhmät määritellään vaihtoehtoisella tavalla. Ratkeavat ryhmät ovat ryhmiä, joilla on äärellisen pituinen subnormaali laskeva jono, jonka jokainen tekijä on vaihdannainen. Toisin sanoen ryhmä G on ratkeava, jos on olemassa subnormaali laskeva jono muotoa

$$G \rhd N_1 \rhd \cdots \rhd N_n \rhd N_{n+1} = \{1_G\},$$

missä N_i/N_{i+1} on vaihdannainen jokaisella i.

Oletetaan, että G on vaihdannainen ryhmä määritelmän 5.8 tavalla, eli on olemassa jokin $k \in \mathbb{N}$, jolla $G^{(k)} = \{1_G\}$. Tällöin kommutaattorialiryhmien jono on äärellinen ja muotoa

$$G \trianglerighteq G' \trianglerighteq \cdots \trianglerighteq G^{(k-1)} \trianglerighteq G^{(k)} = \{1_G\},$$

missä $G^{(i)}/G^{(i+1)} = G^{(i)}/\left(G^{(i)}\right)' = \left(G^{(i)}\right)_{ab}$ on vaihdannainen jokaisella i.

Näin ollen jos G on ratkeava määritelmän 5.8 tavalla, niin G on ratkeava myös tällä vaihtoehtoisella tavalla.

5.3 Nilpotentit ryhmät

Seuraavaksi esitellään nilpotentit ryhmät. Nilpotentit ryhmät ovat ryhmiä, joilla on äärellinen alempi keskusjono.

Määritelmä 5.13 (Alempi keskusjono)**.** Ryhmän G *alempi keskusjono* on jono

$$C^1G \trianglerighteq C^2G \trianglerighteq \cdots \trianglerighteq C^nG \trianglerighteq \ldots,$$

missä

$$C^1G = G, \ C^{n+1}G = [C^nG, G].$$

Huomautus. Tällöin erityisesti $C^2G = [G, G] = G'$.

Lause 5.14. C^kG on ryhmän G karakteristinen aliryhmä jokaisella k. Erityisesti C^kG on ryhmän G normaali aliryhmä jokaisella k.

Todistus. Todistetaan väite induktiolla. Jos $k = 1$, niin jokaisella automorfismilla φ pätee $\varphi(C^1G) = \varphi(G) = G = C^1G$. Siispä C^1G on ryhmän G karakteristinen aliryhmä.

Oletetaan sitten, että kaikilla $k \leq n$ pätee, että C^kG on ryhmän G karakteristinen aliryhmä. Näytetään, että tällöin myös $C^{n+1}G$ on ryhmän G karakteristinen aliryhmä. Olkoon $\varphi \in \mathrm{Aut}(G)$ ja merkitään $S = \{[x, y] \mid x \in C^nG, y \in G\}$. Tällöin S virittää joukon $C^{n+1}G$.

Oletetaan, että $[x,y] \in S$. Nyt $\varphi([x,y]) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}$, missä $\varphi(x)$, $\varphi(x)^{-1} \in C^nG$ ja $\varphi(y), \varphi(y)^{-1} \in G$. Näin ollen $\varphi([x,y]) \in C^{n+1}G$ kaikilla $[x,y] \in S$. Näin ollen $\varphi(C^{n+1}G) \subset C^{n+1}G$.

Toisaalta jos $x \in C^nG$, niin induktio-oletuksen nojalla on olemassa sellainen $h \in C^nG$, että $\varphi(h) = x$. Jos $y \in G$, niin on olemassa $g \in G$, jolla $\varphi(g) = y$. Tällöin

$$xyx^{-1}y^{-1} = \varphi(h)\varphi(g)\varphi(h)^{-1}\varphi(g)^{-1} = \varphi(hgh^{-1}g^{-1}) = \varphi([h,g]),$$

missä $h \in C^nG$ ja $g \in G$. Siispä $C^{n+1}G \subset \varphi(C^{n+1}G)$. Näin ollen C^kG on ryhmän G karakteristinen aliryhmä kaikilla k. Jokainen karakteristinen aliryhmä on normaali, joten C^kG on normaali ryhmän G aliryhmä kaikilla k. $\square$

Määritelmä 5.15 (Nilpotentti)**.** Ryhmä G on *k-nilpotentti*, jos on olemassa sellainen $k \in \mathbb{N}$, että $C^{k+1}G = \{1_G\}$. Pienintä k, jolla G on nilpotentti, kutsutaan ryhmän G *nilpotenssiluokaksi*.

Esimerkki 5.16. (1) Olkoon $G \neq \emptyset$ vaihdannainen. Tällöin lauseen 5.3 nojalla $C^2G = G' = [G,G] = \{1_G\}$. Siis vaihdannaiset ryhmät ovat nilpotentteja ja niiden nilpotenssiluokka on 1.

(2) Eräs tyypillinen esimerkki nilpotentista ryhmästä on *diskreetti Heisenbergin ryhmä* $\mathrm{H}_3(\mathbb{Z})$, joka koostuu 3×3-matriiseista, jotka ovat muotoa

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, \ a, b, c \in \mathbb{Z}.$$

Aliryhmän C^2G virittäjät ovat muotoa $[g,h]$, missä $g, h \in \mathrm{H}_3(\mathbb{Z})$. Tutkitaan mielivaltaista tällaista virittäjää, kun alkiot g ja h ovat muotoa

$$g = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \quad \text{ja} \quad h = \begin{pmatrix} 1 & d & f \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix}.$$

Näiden alkioiden kommutaattorille pätee

$$\begin{aligned}
[g,h] &= \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & f \\ 0 & 1 & e \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ab-c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -d & de-f \\ 0 & 1 & -e \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & ae-bd \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\end{aligned}$$

Näin ollen aliryhmä $C^2H_3(\mathbb{Z})$ on epätriviaali ryhmä.

Määritelmän nojalla aliryhmän $C^3H_3(\mathbb{Z})$ virittäjät ovat muotoa $[x,y]$, missä $x \in C^2H_3(\mathbb{Z})$ ja $y \in H_3(\mathbb{Z})$. Tarkastellaan aluksi tilannetta $x = [g,h]$, jolloin aiemmilla merkinnöillä

$$x = \begin{pmatrix} 1 & 0 & ae-bd \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

ja merkitään

$$y = \begin{pmatrix} 1 & y_1 & y_3 \\ 0 & 1 & y_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Nyt

$$\begin{aligned}
[x,y] &= \begin{pmatrix} 1 & 0 & ae-bd \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y_1 & y_3 \\ 0 & 1 & y_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & bd-ae \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -y_1 & y_3 \\ 0 & 1 & -y_2 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},
\end{aligned}$$

eli $[g,h]y = y[g,h]$. Tällöin myös mielivaltaisella $x' \in C^2H_3(\mathbb{Z})$ pätee $x'y = yx'$, eli $[x',y] = I_{3\times 3}$. Tästä seuraa, että aliryhmä $C^3H_3(\mathbb{Z})$ on triviaali. Näin ollen diskreetillä Heisenbergin ryhmällä $H_3(\mathbb{Z})$ on alempi keskusjono muotoa

$$H_3(\mathbb{Z}) \trianglerighteq C^2H_3(\mathbb{Z}) \trianglerighteq C^3H_3(\mathbb{Z}) = \{I_{3\times 3}\},$$

joten $H_3(\mathbb{Z})$ on nilpotentti.

Esimerkki 5.17. Esimerkissä 5.16 osoitettiin, että jokainen kommutaattorialiryhmän $(H_3(\mathbb{Z}))' = C^2 H_3(\mathbb{Z})$ alkio kommutoi jokaisen ryhmän $H_3(\mathbb{Z})$ alkion kanssa. Erityisesti tästä seuraa, että $(H_3(\mathbb{Z}))'$ on vaihdannainen ryhmä. Näin ollen $(H_3(\mathbb{Z}))^{(2)}$ on triviaali, joten diskreetti Heisenberg ryhmä on ratkeava.

Esimerkissä 5.17 osoitettiin, että nilpotentti ryhmä $H_3(\mathbb{Z})$ on ratkeava. Tämä pätee itse asiassa kaikille nilpotenteille ryhmille, eli jokainen nilpotentti ryhmä on ratkeava.

Lause 5.18. Jokainen nilpotentti ryhmä on ratkeava.

Todistus. Osoitetaan induktiolla, että jokaisella $i \geq 0$ ryhmä $G^{(i)}$ on ryhmän $C^{i+1}G$ aliryhmä. Jos $i = 0$, niin $G^{(0)} = G = C^1 G$, joten alkutapaus on selvä. Oletetaan sitten, että jokaisella $k \leq n$ pätee, että $G^{(k)} \leqslant C^{k+1}G$. Määritelmän nojalla $G^{(n+1)} = [G^{(n)}, G^{(n)}]$. Tarkastellaan ryhmän $G^{(n+1)}$ virittäjäalkiota $[x, y]$, missä $x, y \in G^{(n)}$. Induktio-oletuksen nojalla $x \in C^{n+1}G$. Tällöin ryhmän $C^{n+2}G$ määritelmän nojalla $[x, y]$ on myös ryhmän $C^{n+2}G$ virittäjäalkio. Tästä seuraa, että $G^{(n+1)} \leqslant C^{n+2}G$.

Näin ollen jokaisella $i \geq 0$ pätee $G^{(i)} \leqslant C^{i+1}G$. Tästä seuraa erityisesti, että jos ryhmä G on k-nilpotentti, niin $G^{(k)} \leqslant C^{k+1}G = \{1_G\}$. Tällöin $G^{(k)} = \{1_G\}$, joten ryhmä G on myös ratkeava. □

Nilpotenteille ryhmille pätevät vastaavat ominaisuudet kuin ratkeaville ryhmille: esimerkiksi nilpotentin ryhmän aliryhmä on nilpotentti ja nilpotentin ryhmän tekijäryhmät ovat nilpotentteja.

Lause 5.19. Nilpotentin ryhmän aliryhmä on myös nilpotentti.

Todistus. Oletetaan, että G on nilpotentti ryhmä ja H sen aliryhmä. On olemassa sellainen $k \in \mathbb{N}$, että $C^{k+1}G = \{1_G\}$. Osoitetaan induktiolla, että $C^i H$ on aliryhmä ryhmälle $C^i G$ kaikilla i. Tapaus $i = 1$ on selvä, sillä oletusten nojalla H on ryhmän G aliryhmä.

Oletetaan sitten, että $C^i H$ on aliryhmä $C^i G$ aliryhmä jollain i. Määritelmän nojalla $C^{i+1}H = [C^i H, H]$. Oletetaan, että $x \in C^i H$ ja $h \in H$. Tällöin $[x, h]$ on ryhmän $C^{i+1}H$ virittäjäalkio ja $[x, h] = xhx^{-1}h^{-1} \in C^{i+1}G$, sillä induktio-oletuksen nojalla $x, x^{-1} \in C^i G$. Tästä seuraa, että $C^i H \leqslant C^i G$.

Jos G on k-nilpotentti, niin $C^{k+1}H \leqslant C^{k+1}G = \{1_G\}$. Näin ollen, jos ryhmä G on nilpotentti, niin sen aliryhmä H on myös nilpotentti. □

Lause 5.20. Nilpotentin ryhmän tekijäryhmä normaalin aliryhmän suhteen on myös nilpotentti.

Todistus. Oletetaan, että G on nilpotentti ryhmä ja N sen normaali aliryhmä. Olkoon $\pi\colon G \to G/N$ tekijähomomorfismi. Aliryhmän N normaaliudesta seuraa, että G/N on ryhmä.

Osoitetaan induktiolla, että $\pi(C^iG) = C^i(G/N)$. Tapaus $i = 1$ on selvä, sillä $\pi(G) = G/N$. Oletetaan sitten, että $\pi(C^iG) = C^i(G/N)$ jollain i. Määritelmän nojalla $C^{i+1}(G/N) = [C^i(G/N), G/N]$.

Tarkastellaan ryhmän $C^{i+1}G$ virittäjäalkiota $[x, g]$, missä $x \in C^iG$, $g \in G$. Tällöin $\pi([x, g]) = \pi(x)\pi(g)\pi(x)^{-1}\pi(g)^{-1} = [\pi(x), \pi(g)] \in C^{i+1}(G/N)$, sillä induktio-oletuksen nojalla $\pi(x) \in C^i(G/N)$. Näin ollen $\pi(C^{i+1}G) \subset C^{i+1}(G/N)$.

Tarkastellaan sitten ryhmän $C^{i+1}(G/N)$ virittäjäalkiota $[xN, gN]$, missä $xN \in C^i(G/N)$ ja $gN \in G/N$. Induktio-oletuksen nojalla $C^i(G/N) = \pi(C^iG)$, joten $xN, x^{-1}N \in \pi(C^iG)$. On siis olemassa jokin $y \in C^iG$, jolla pätee $\pi(y) = xN$ ja $\pi(y^{-1}) = \pi(y)^{-1} = x^{-1}N$. Nyt

$$[xN, gN] = xNgNx^{-1}Ng^{-1}N = \pi(y)\pi(g)\pi(y)^{-1}\pi(g)^{-1} = \pi(ygy^{-1}g^{-1}),$$

missä $ygy^{-1}g^{-1} = [y, g] \in C^{i+1}G$. Näin ollen $C^{i+1}(G/N) \subset \pi(C^{i+1}G)$.

Näin ollen jokaisella $i \geq 1$ pätee $\pi(C^iG) = C^i(G/N)$. Tästä seuraa, että jos ryhmä G on k-nilpotentti, niin $C^{k+1}(G/N) = \pi(C^{k+1}G) = \pi(1_G) = 1_{G/N}$, eli tekijäryhmä G/N on nilpotentti. □

5.4 Polysykliset ryhmät

Määritelmä 5.21. Olkoon G ryhmä. Jos on olemassa $n \in \mathbb{N}$, jolla

$$G = N_0 \rhd N_1 \rhd \cdots \rhd N_n \rhd N_{n+1} = \{1_G\}$$

ja N_i/N_{i+1} on syklinen kaikilla $i \geq 0$, niin ryhmää G kutsutaan *polysykliseksi*, ja tätä jonoa kutsutaan *ryhmän G sykliseksi jonoksi*. Syklisen jonon *pituudeksi* kutsutaan sen epätriviaalien ryhmien lukumäärää, ja polysyklisen ryhmän G *pituus* $\ell(G)$ on lyhin mahdollinen syklisen jonon pituus. Jos N_i/N_{i+1} on ääretön syklinen jokaisella $i \geq 0$, niin ryhmä G on poly $-C_\infty$ *ryhmä*, ja jonoa kutsutaan C_∞- *jonoksi*.

Esimerkki 5.22. Jokainen äärellisesti viritetty vaihdannainen ryhmä on polysyklinen. Olkoon G vaihdannainen ja $S = \{s_1, \ldots, s_n\}$ äärellinen virittäjäjoukko. Muodostetaan nyt ryhmälle G syklinen jono seuraavasti.

Ryhmän G vaihdannaisuudesta seuraa, että jokainen $g \in G$ on muotoa $g = s_1^{k_1} \cdots s_n^{k_n}$, missä $k_i \in \mathbb{Z}$. Olkoon N_1 joukon $\{s_2, \ldots, s_n\}$ virittämä ryhmän G aliryhmä. Tällöin vaihdannaisuuden nojalla N_1 on normaali ryhmässä G. Oletetaan, että $gN_1 \in G/N_1$, missä $g = s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} \in G$. Tällöin $g \in s_1^{k_1} N_1$, eli $gN = s_1^{k_1} N_1$. Näin ollen ryhmä G/N_1 on syklinen ja sen virittäjä on $s_1 N_1$.

Olkoon N_2 joukon $\{s_3, \ldots, s_n\}$ virittämä N_1 aliryhmä. Tällöin $N_2 \lhd N_1$ ja tekijäryhmä N_1/N_2 on syklinen. Tekijäryhmän N_1/N_2 virittäjä on alkio $s_2 N_2$. Jos nimittäin $hN_2 \in N_1/N_2$, missä $h = s_2^{k_2} s_3^{k_3} \cdots s_n^{k_n} \in N_1$, niin $hN_1 = s_2^{k_2} N_2$.

Vastaavasti määritellään N_i joukon $\{s_{i+1}, \ldots, s_n\}$ virittämäksi ryhmän N_{i-1} aliryhmäksi. Tällöin tekijäryhmä N_{i-1}/N_i on syklinen ja sen virittäjäalkio on $s_i N_i$. Aliryhmä N_{n-1} on alkion s_n virittämä ryhmä eli syklinen. Tällöin myös $N_{n-1}/\{1_G\}$ on syklinen.

Näin ollen jono

$$G \rhd N_1 \rhd \cdots \rhd N_{n-1} \rhd \{1_G\}$$

on ryhmän G syklinen jono ja ryhmä G on polysyklinen.

Lause 5.23. Polysykliset ryhmät ovat ratkeavia.

Todistus. Todistetaan väite induktiolla syklisen jonon pituuden suhteen. Oletetaan ensin, että G on ryhmä, jolla on syklinen jono muotoa

$$G \trianglerighteq \{1_G\}.$$

Nyt $G \cong G/\{1_G\}$ on syklisenä ryhmänä vaihdannainen. Tällöin $G^{(1)} = G' = \{1_G\}$, joten ryhmä G on ratkeava.

Oletetaan sitten, että jokainen polysyklinen ryhmä, jonka syklisen jonon pituus on korkeintaan n, on myös ratkeava. Olkoon G polysyklinen ryhmä, jonka syklisen jonon pituus on $n+1$. Tällöin ryhmällä G on syklinen jono muotoa

$$G \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_n \trianglerighteq N_{n+1} = \{1_G\}.$$

Induktio-oletuksen nojalla aliryhmä N_1 on ratkeava. Tekijäryhmä G/N_1 on oletusten nojalla syklinen ryhmä eli myös vaihdannainen. Näin ollen ryhmä G/N_1 on vaihdannaisena ryhmänä ratkeava. Lauseen 5.12 nojalla ryhmä G on ratkeava.

Näin ollen jokainen polysyklinen ryhmä on ratkeava. $\square$

Lause 5.24 (Polysyklisen ryhmän virittäjäjoukko)**.** Olkoon G polysyklinen ryhmä, jolla on syklinen jono, jonka pituus on n. Oletetaan, että $t_i \in N_i$, ovat sellaisia, että $t_i N_{i+1}$ on tekijäryhmän N_i/N_{i+1} virittäjä, $i \geq 0$. Tällöin jokainen $g \in G$ voidaan kirjoittaa muodossa $t_0^{k_0} \dots t_{n-1}^{k_{n-1}}$, missä $k_0, \dots, k_{n-1} \in \mathbb{Z}$.

Todistus. Todistetaan väite induktiolla syklisen jonon pituuden n suhteen. Jos $n = 1$, niin ryhmällä G on syklinen jono, joka on muotoa

$$G \rhd \{1_G\}.$$

Koska tällöin $G/\{1_G\} \cong G$ on syklinen, niin on olemassa sellainen $t \in G$, että $t\{1_G\}$ virittää tekijäryhmän $G/\{1_G\}$. Tästä seuraa, että alkio t virittää ryhmän G, joten jokainen $g \in G$ voidaan kirjoittaa muodossa t^k, missä $k \in \mathbb{Z}$.

Oletetaan sitten, että väite pätee kaikilla $k \leq n$. Olkoon G polysyklinen ryhmä, jolla on $(n+1)$-pituinen syklinen jono. Syklinen jono on siis muotoa

$$G \rhd N_1 \rhd \cdots \rhd N_n \rhd N_{n+1} = \{1\}.$$

Ryhmän G normaalilla aliryhmällä N_1 on syklinen jono, jonka pituus on n, joten jokainen ryhmän N_1 alkio voidaan kirjoittaa muodossa $t_1^{k_1} \cdots t_n^{k_n}$, missä $t_i \in N_i$ on sellainen, että $t_i N_{i+1}$ virittää ryhmän N_i/N_{i+1} ja $k_i \in \mathbb{Z}$.

Oletusten nojalla ryhmä G/N_1 on syklinen, joten on olemassa jokin sellainen $t_0 \in G$, että $t_0 N_1$ virittää ryhmän G/N_1. Oletetaan, että $g \in G$. Nyt $gN_1 = t_0^{k_0} N_1$ jollain $k_0 \in \mathbb{Z}$, mikä tarkoittaa, että $(t_0^{k_0})^{-1} g \in N_1$. Siis $(t_0^{k_0})^{-1} g = t_1^{k_1} \cdots t_n^{k_n}$, mistä saadaan, että $g = t_0^{k_0} t_1^{k_1} \cdots t_n^{k_n}$. $\square$

Lause 5.25. Jokainen polysyklisen ryhmän aliryhmä on polysyklinen ja siten myös äärellisesti viritetty.

Todistus. Oletetaan, että G on polysyklinen ryhmä, jolla on syklinen jono muotoa

$$G \rhd N_1 \rhd \cdots \rhd N_n \rhd \{1_G\},$$

ja olkoon H ryhmän G aliryhmä. Tällöin ryhmälle H voidaan muodostaa syklinen jono ryhmistä $H \cap N_i$.

Ensimmäisestä isomorfialauseesta seuraa, että $H \cap N_{i+1} = (H \cap N_i) \cap N_{i+1} \lhd H \cap N_i$. Lisäksi 1. isomorfialauseesta seuraa, että

$$\begin{aligned}(H \cap N_i)/(H \cap N_{i+1}) &= (H \cap N_i)/(H \cap N_i \cap N_{i+1}) \\ &\cong (H \cap N_i)N_{i+1}/N_{i+1} \leq N_i/N_{i+1}.\end{aligned}$$

Näin ollen $(H \cap N_i)/(H \cap N_{i+1})$ on syklisen ryhmän aliryhmänä syklinen.

Siispä ryhmällä H on syklinen jono, joka on muotoa

$$H \triangleright H \cap N_1 \triangleright \cdots \triangleright H \cap N_n \triangleright \{1_H\},$$

ja H on polysyklinen. $\square$

Lause 5.26. Jos N on polysyklisen ryhmän G normaali aliryhmä, niin G/N on polysyklinen.

Todistus. Todistus tehdään induktiolla polysyklisen ryhmän pituuden $\ell(G) = n$ suhteen.

Alkuaskeleessa $n = 1$ saadaan, että ryhmällä G on syklinen jono, joka on muotoa

$$G \triangleright \{1_G\}.$$

Tällöin $G \cong G/\{1_G\}$ on syklinen. Näin ollen on olemassa jokin sellainen $t \in G$, että jokainen $g \in G$ on muotoa t^k, missä $k \in \mathbb{Z}$. Oletetaan sitten, että N on ryhmän G normaali aliryhmä. Tällöin G/N on ryhmä. Nyt ryhmän G syklisyydestä seuraa, että mielivaltainen sivuluokka ryhmässä G/N on muotoa t^kN jollain $k \in \mathbb{Z}$. Näin ollen alkio tN virittää ryhmän G/N, joten tekijäryhmä G/N syklinen. Tällöin ryhmälle G/N voidaan tehdä syklinen jono, joka on muotoa

$$G/N \triangleright \{1_{G/N}\}.$$

Ryhmä G/N on näin ollen polysyklinen.

Tehdään sitten induktio-oletus, että jokaiselle polysykliselle ryhmälle, jonka pituus on korkeintaan n, pätee, että myös tekijäryhmä normaalin aliryhmän suhteen on polysyklinen. Tutkitaan sitten ryhmää G, jolle pätee $\ell(G) = n+1$. Nyt ryhmällä G on syklinen jono, joka on muotoa

$$G \triangleright N_1 \triangleright \cdots \triangleright N_n \triangleright N_{n+1} = \{1_G\}.$$

Olkoon N_1 jonon ensimmäinen termi, joka on eri kuin G. Ryhmä N_1 on polysyklinen ja $\ell(N_1) \leq n$. Oletetaan, että N on normaali ryhmän G aliryhmä. Tällöin 1. isomorfialauseen nojalla $N_1 \cap N$ on normaali ryhmän N_1 aliryhmä, ja lisäksi $N_1/(N_1 \cap N) \cong N_1N/N$. Induktio-oletuksen nojalla N_1N/N on polysyklinen, joten ryhmällä N_1N/N on jokin syklinen jono

$$N_1N/N \triangleright \bar{N}_1 \triangleright \cdots \triangleright \bar{N}_m = \{\bar{1}\},$$

missä $\bar{1}$ on ryhmän N_1N/N neutraalialkio N.

Ryhmän N normaaliudesta seuraa, että N_1N on ryhmän G aliryhmä. Tämä on lisäksi normaali aliryhmä, sillä kaikilla $g \in G$ ja $m = n_1n \in N_1N$ pätee $gmg^{-1} = gn_1g^{-1}gng^{-1} \in N_1N$. Nyt 2. isomorfialauseen nojalla N_1N/N on normaali ryhmässä G/N ja

$$(G/N)/(N_1N/N) \cong G/N_1N.$$

Oletuksien nojalla G/N_1 on syklinen, joten G/N_1N on syklinen. Näin ollen ryhmällä G/N on syklinen jono muotoa

$$G/N \triangleright N_1N/N \triangleright \bar{N}_1 \triangleright \cdots \triangleright \bar{N}_m = \{\bar{1}\}.$$

□

Lause 5.27. Jos N on ryhmän G normaali aliryhmä ja sekä N että G/N ovat polysyklisiä, niin G on polysyklinen.

Todistus. Olkoon G ryhmä ja N sen normaali aliryhmä. Oletetaan, että ryhmällä G/N on syklinen jono muotoa

$$G/N = Q_0 \triangleright Q_1 \triangleright \cdots \triangleright Q_n = \{1_{G/N}\},$$

ja ryhmällä N on syklinen jono muotoa

$$N = N_0 \triangleright \cdots \triangleright N_k = \{1_G\}.$$

Merkitään $H_i = \pi^{-1}(Q_i)$, missä $\pi\colon G \to G/N$ on tekijähomomorfismi. Tällöin $\pi^{-1}(Q_{i+1}) \leq \pi^{-1}(Q_i)$ jokaisella i. Oletetaan, että $q_{i+1} \in \pi^{-1}(Q_{i+1})$ ja $q_i \in \pi^{-1}(Q_i)$. Nyt $\pi(q_iq_{i+1}q_i^{-1}) \in Q_{i+1}$, joten $q_iq_{i+1}q_i^{-1} \in \pi^{-1}(Q_{i+1})$. Näin ollen normaaliuskriteerin nojalla $\pi^{-1}(Q_{i+1})$ on normaali ryhmässä $\pi^{-1}(Q_i)$. Siis $H_i \triangleright H_{i+1}$ kaikilla i.

Osoitetaan vielä, että H_i/H_{i+1} on syklinen jokaisella i. Oletusten nojalla Q_{i+1} on normaali ryhmässä Q_i ja $\{1_{G/N}\} = N$ on normaali ryhmässä Q_{i+1}. Nyt 2. isomorfialauseen nojalla ryhmä Q_{i+1}/N on normaali ryhmässä Q_i/N ja

$$(Q_i/N) \Big/ (Q_{i+1}/N) \cong Q_i/Q_{i+1}.$$

Olkoon $\pi|_{H_i}\colon H_i \to Q_i/N$ tekijähomomorfismin π rajoittuma joukkoon H_i, ja olkoon $\pi'\colon Q_i/N \to (Q_i/N)/(Q_{i+1}/N)$ tekijähomomorfismi. Tällöin $\pi' \circ \pi|_{H_i}$ on surjektio, joten homomorfialauseen nojalla $H_i/\ker(\pi' \circ \pi|_{H_i}) \cong (Q_i/N)/(Q_{i+1}/N)$. Saadaan alla oleva kommutoiva kaavio:

$$\begin{tikzcd}
H_i \arrow[r, "\pi|_{H_i}"] \arrow[dr, "q"'] & Q_i/N \arrow[r, "\pi'"] & (Q_i/N)/(Q_{i+1}/N) \\
& H_i/\ker(\pi' \circ \pi|_{H_i}) \arrow[ur, "\cong"] &
\end{tikzcd}$$

Jos $g \in \ker(\pi' \circ \pi|_{H_i})$, eli $\pi' \circ \pi|_{H_i}(g) \subset Q_{i+1}/N$, niin $\pi|_{H_i}(g) \in Q_{i+1}/N$. Näin ollen $g \in \pi^{-1}(Q_{i+1}) = H_{i+1}$. Toisaalta, jos $h \in H_{i+1}$, niin $\pi|_{H_i}(h) \in Q_{i+1}/N$, joten $\pi' \circ \pi|_{H_i}(h) = Q_{i+1}/N \in \ker(\pi' \circ \pi|_{H_i})$. Näin ollen $H_{i+1} = \ker(\pi' \circ \pi|_{H_i})$, joten $H_i/H_{i+1} \cong (Q_i/N)/(Q_{i+1}/N) \cong Q_i/Q_{i+1}$. Oletusten nojalla Q_i/Q_{i+1} on syklinen, joten myös H_i/H_{i+1} on syklinen.

Ryhmälle G saadaan siis syklinen jono muotoa

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = N = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_k = \{1_G\},$$

joten G on polysyklinen. □

Lauseen 5.27 avulla voidaan osoittaa, että jokainen äärellisesti viritetty nilpotentti ryhmä on polysyklinen.

Lause 5.28. Jokainen äärellisesti viritetty nilpotentti ryhmä on polysyklinen.

Todistus. Osoitetaan väite induktiolla nilpotenssiluokan suhteen. Oletetaan, että G on äärellisesti viritetty 1-nilpotentti ryhmä. Tällöin $C^2G = G' = \{1_G\}$, joten G on vaihdannainen. Tällöin ryhmä G on äärellisesti viritettynä ja vaihdannaisena ryhmänä polysyklinen.

Oletetaan sitten, että jokainen äärellisesti viritetty k-nilpotentti ryhmä, missä $k \leq n$, on polysyklinen. Olkoon G äärellisesti viritetty $(n+1)$-nilpotentti ryhmä. Tällöin $C^{n+2}G = [C^{n+1}G, G] = \{1_G\}$ ja ryhmällä G on subnormaali laskeva jono muotoa

$$G \trianglerighteq C^2G \trianglerighteq \cdots \trianglerighteq C^{n+1}G \trianglerighteq C^{n+2}G = \{1_G\}.$$

Koska G on $(n+1)$-nilpotentti, jokainen aliryhmän $C^{n+1}G$ alkio kommutoi jokaisen ryhmän G alkion kanssa. Tästä seuraa, että aliryhmä $C^{n+1}G$ on vaihdannainen. Tutkitaan ryhmän G aliryhmää C^2G. Olkoon $[x,g] \in C^{n+1}(C^2G)$ virittäjäalkio. Tällöin $x \in C^n(C^2G) \leqslant C^nG$ ja $g \in C^2G \leqslant G$, joten $[x,g] \in [C^nG, G] = C^{n+1}G$. Nyt ryhmän $C^{n+1}G$ vaihdannaisuudesta seuraa, että $[x,g] = 1_G$. Tästä seuraa, että $C^{n+1}(C^2G) = \{1_G\}$, eli C^2G on n-nilpotentti. Induktio-oletuksen nojalla C^2G on polysyklinen.

Tekijäryhmä $G/C^2G = G/G' = G_{ab}$ on äärellisesti viritettynä ja vaihdannaisena ryhmänä polysyklinen. Nyt lauseen 5.27 nojalla ryhmä G on polysyklinen.

Näin ollen jokainen äärellisesti viritetty nilpotentti ryhmä on polysyklinen. $\square$

Esimerkki 5.29. Diskreetti Heisenberg ryhmä $H_3(\mathbb{Z})$ on äärellisesti viritettynä nilpotenttina ryhmänä polysyklinen. Esimerkissä 5.16 osoitettiin, että ryhmällä $H_3(\mathbb{Z})$ on alempi keskusjono muotoa

$$H_3(\mathbb{Z}) \trianglerighteq C^2H_3(\mathbb{Z}) \trianglerighteq C^3H_3(\mathbb{Z}) = \{I_{3\times3}\},$$

ja lisäksi ryhmällä $H_3(\mathbb{Z})$ on äärellinen virittäjäjoukko $\{x, y, z\}$, missä

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{ja} \quad z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Nyt lauseen 5.28 nojalla $H_3(\mathbb{Z})$ on polysyklinen. Tämä voidaan osoittaa myös seuraavasti. Ryhmät C^kG ovat äärellisesti viritettyjä jokaisella k, jos G on äärellisesti viritetty (ks. [2, corollary 13.45]). Näin ollen $C^2H_3(\mathbb{Z})$ on äärellisesti viritettynä ja vaihdannaisena ryhmänä polysyklinen. Tekijäryhmä $H_3(\mathbb{Z})/C^2H_3(\mathbb{Z}) = H_3(\mathbb{Z})/\left(H_3(\mathbb{Z})\right)' = H_3(\mathbb{Z})_{ab}$ on vaihdannainen ja äärellisesti viritetty, joten myös se on polysyklinen. Lauseen 5.27 nojalla diskreetti Heisenbergin ryhmä $H_3(\mathbb{Z})$ on polysyklinen.

Luku 6

Milnorin lause

Tässä luvussa todistetaan Milnorin lause, jonka mukaan jokainen äärellisesti viritetty ratkeava ryhmä joko kasvaa eksponentiaalisesti tai on polysyklinen. Tähän lukuun on koottu ryhmien kasvuun, polysyklisiin ryhmiin ja ryhmien esityksiin liittyviä lauseita, joita hyödynnetään Milnorin lauseen todistuksessa. Luvussa 2.3 esitellyt lyhyet eksaktit jonot tulevat käyttöön itse Milnorin lauseen todistuksessa ja lauseissa 6.2 ja 6.4.

Luvun lopussa esitellään Wolfin lause ja yhdistetään Milnorin ja Wolfin lauseet yhdeksi lauseeksi, joka luokittelee äärellisesti viritettyjen ratkeavien ryhmien kasvun.

Lause 6.1. Jokaisella polysyklisellä ryhmällä on äärellinen esitys.

Todistus. Osoitetaan väite induktiolla lyhimmän syklisen jonon pituuden suhteen. Olkoon aluksi G polysyklinen ryhmä, jolla on syklinen jono muotoa

$$G = N_0 \triangleright N_1 = \{1_G\}.$$

Tällöin G on syklinen ryhmä. Olkoon $t \in G$ ryhmän G virittäjä. Jos on olemassa jokin sellainen $k \in \mathbb{Z}$, että $t^k = 1_G$, niin ryhmällä G on äärellinen esitys $\langle t \mid t^k \rangle$. Jos puolestaan G on ääreton syklinen, niin ryhmällä G on esitys muotoa $\langle t \mid \, \rangle$.

Oletetaan sitten, että väite pätee kaikille polysyklisille ryhmille, joiden syklisen jonon lyhin pituus on korkeintaan n. Oletetaan, että G on ryhmä, jonka syklisen jonon lyhin pituus on $n+1$. Tällöin ryhmällä G on polysyklinen jono muotoa

$$G = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_n \triangleright N_{n+1} = \{1_G\}.$$

Tällöin ryhmä G/N_1 on syklisenä ryhmänä myös polysyklinen ryhmä, jonka syklisen jonon pituus on 1. Lisäksi ryhmä N_1 on polysyklinen ryhmä, jolla on syklinen jono, jonka lyhin pituus on n. Nyt induktio-oletuksen nojalla aliryhmällä N_1 ja tekijäryhmällä G/N_1 on äärelliset esitykset. Näin ollen lauseen 3.12 nojalla myös ryhmällä G on äärellinen esitys. $\square$

Lemma 6.2. Olkoon K äärellisesti viritetty ryhmä ja olkoon

$$1 \to N \to K \xrightarrow{\pi} G \to 1$$

lyhyt eksakti jono. Jos ryhmällä G on äärellinen esitys, niin $N = \langle\langle T \rangle\rangle$, missä $T = \{n_1, \dots, n_k\} \subset N$.

Todistus. Olkoon S ryhmän K äärellinen virittäjäjoukko. Tällöin $\bar{S} = \pi(S)$ on ryhmän G äärellinen virittäjäjoukko. Oletusten nojalla G on äärellisesti esitetty. Koska lauseen 3.11 nojalla äärellinen esitys ei riipu virittäjäjoukosta, on olemassa sellaiset aakkoston $\bar{S} \cup \bar{S}^{-1}$ sanat $\bar{R} = \{\bar{r}_1, \dots, \bar{r}_k\}$, että $\langle S | \bar{R} \rangle$ on ryhmän G äärellinen esitys. Jokaista sanaa $\bar{r}_i$ vastaa aakkoston $S \cup S^{-1}$ sana seuraavasti. Jos $\bar{r}_i = \pi(s_1) \cdots \pi(s_l)$, niin ryhmän G alkiona $\pi_{\bar{S}}(\bar{r}_i) = \pi(s_1) \cdots \pi(s_l) = \pi(s_1 \cdots s_l)$. Tässä $s_1 \cdots s_l = \pi_S(r_i)$, missä $r_i = s_1 \cdots s_l$ aakkoston $S \cup S^{-1}$ sana. Joukkoa $\bar{R} \subset F(\bar{S})$ vastaa siis joukko $R = \{r_1, \dots, r_k\} \subset F(S)$.

Jokaiselle $r_i \in R$ pätee $\pi(\pi_S(r_i)) = \pi_{\bar{S}}(\bar{r}_i) = 1_G$. Erityisesti $\pi_S(r_i) \in \ker \pi = N$. Valitaan $n_i = \pi_S(r_i)$. Olkoon sitten $n \in N$ jokin alkio. Koska π_S on surjektio, on olemassa aakkoston $S \cup S^{-1}$ sana w_S, jolla $n = \pi_S(w_S)$. Tällöin $\pi(\pi_S(w_S)) = \pi(n) = 1_G$. Sanaa w_S vastaavalle aakkoston $\bar{S} \cup \bar{S}^{-1}$ sanalle $w_{\bar{S}}$ pätee tällöin $\pi_{\bar{S}}(w_{\bar{S}}) = \pi(\pi_S(w_S)) = 1_G$, mistä seuraa, että sana $w_{\bar{S}}$ on äärellinen tulo sanojen $\bar{r_1}, \dots, \bar{r}_k$ konjugaatteja. Tästä seuraa, että ryhmässä $F(S)$ sana w_S on äärellinen tulo sanojen $r_1, \dots, r_k$ konjugaatteja. Tällöin n on äärellinen tulo alkioiden $n_1, \dots, n_k$ konjugaatteja, sillä $n_i = \pi_S(r_i)$ jokaisella $1 \leq i \leq k$. Näin ollen $N = \langle\langle T \rangle\rangle$, missä $T = \{n_1, \dots, n_k\} \subset N$. $\square$

Lause 6.3. Olkoon G ryhmä, jolla on äärellinen virittäjäjoukko S. Jos ryhmä G kasvaa subeksponentiaalisesti, niin kaikilla alkioilla $\beta_1, \dots, \beta_l, g \in G$ joukko $\{g^k \beta_i g^{-k} \mid k \in \mathbb{Z},\ i = 1, \dots, l\}$ virittää äärellisviritteisen ryhmän G aliryhmän N.

Todistus. Olkoon N joukon $\{g^k \beta_i g^{-k} \mid k \in \mathbb{Z},\ i = 1, \dots, l\}$ virittämä ryhmä. Halutaan osoittaa, että N on äärellisesti viritetty. Olkoon N_i joukon $\{g^k \beta_i g^{-k} \mid k \in \mathbb{Z}\}$

virittämä ryhmä jokaisella $i \in \{1, \dots, l\}$. Tällöin $N = \langle N_1, \dots, N_l \rangle$, joten riittää tarkastella tilannetta $l = 1$. Jos nimittäin ryhmät N_i ovat äärellisesti viritettyjä jokaisella $i = 1, \dots, l$, niin tällöin myös N on äärellisesti viritetty.

Koska G on subeksponentiaalisesti kasvava ryhmä, niin ryhmän G kasvuvakiolle pätee $\gamma_S = \lim_{n\to\infty} \mathcal{B}_S(n)^{\frac{1}{n}} = 1$. Oletetaan, että $\alpha, g \in G$ ja merkitään $\alpha_k = g^k \alpha g^{-k}$. Olkoon N joukon $\{\alpha_k \mid k \in \mathbb{Z}\}$ virittämä ryhmä. Halutaan osoittaa, että vain äärellinen määrä joukon $\{\alpha_k \mid k \in \mathbb{Z}\}$ alkioita virittää ryhmän N.

Määritellään jokaisella $m \geq 0$ kuvaus

$$\mu_m : \prod_{i=0}^{m} \{0, 1\} \to G,\ (s_0, \dots, s_m) \mapsto g\alpha^{s_0} \cdots g\alpha^{s_m}.$$

Tarkastellessa kuvauksia μ_m tarkemmin huomataan, että μ_m ei voi olla injektio jokaisella m. Jos g ja α ovat joukon G virittäjäalkioita, niin $|g|_S = 1$ ja $|\alpha|_S = 1$. Tällöin erityisesti $g\alpha^{s_0} \cdots g\alpha^{s_m} \in \bar{B}_S(1, 2(m+1))$. Jos μ_m on injektio jokaisella m, niin on olemassa 2^{m+1} kappaletta muotoa $g\alpha^{s_0} \cdots g\alpha^{s_m}$ olevia tuloja, sillä mahdollisia jonoja $(s_0, \dots, s_m)$ on 2^{m+1} kappaletta. Tällöin $\operatorname{card} \bar{B}_S(1, 2(m+1)) \geq 2^{m+1}$. Tämä on ristiriidassa sen kanssa, että ryhmän G oletettiin kasvavan subeksponentiaalisesti.

Näin ollen μ_m ei voi olla injektio jokaisella m. On siis olemassa jokin m ja sellaiset kaksi eri jonoa $(s_0, \dots, s_m)$ ja $(t_0, \dots, t_m)$, että

$$\mu_m(s_0 \dots, s_m) = g\alpha^{s_0} \cdots g\alpha^{s_m} = g\alpha^{t_0} \cdots g\alpha^{t_m} = \mu_m(t_0, \dots, t_m). \tag{6.3.1}$$

Valitaan nyt m pienimmäksi luvuksi, jolla ominaisuus (6.3.1) pätee joillain eri jonoilla $(s_0, \dots, s_m)$ ja $(t_0, \dots, t_m)$. Nyt $s_i \neq t_i$ ainakin yhdellä $0 \leq i \leq m$. Jos pätee, että $s_0 = t_0$, niin yhtälö (6.3.1) voidaan muokata muotoon

$$g\alpha^{s_1} \cdots g\alpha^{s_m} = g\alpha^{t_1} \cdots g\alpha^{t_m},$$

jolloin m ei olisikaan pienin luku, jolla ominaisuus (6.3.1) pätee. Näin ollen $s_0 \neq t_0$. Vastaavasti voidaan päätellä, että $s_m \neq t_m$. Näin ollen, jos m on pienin luku, jolla ominaisuus (6.3.1) pätee, niin $s_0 \neq t_0$ ja $s_m \neq t_m$.

Osoitetaan seuraavaksi, että jokaisella m pätee yhtälö

$$g\alpha^{s_0} \cdots g\alpha^{s_m} = \alpha_1^{s_0} \alpha_2^{s_1} \cdots \alpha_{m+1}^{s_m} g^{m+1}.$$

Jos $m = 0$, niin joko $g\alpha^{s_0} = g\alpha^0 = g = \alpha_1^{s_0} g$ tai $g\alpha^{s_0} = g\alpha^1 = g\alpha g^{-1} g = \alpha_1^{s_0} g$. Yhtälö siis pätee tapauksessa $m = 0$. Oletetaan sitten, että yhtälö pätee n-pituisilla jonoilla $(s_0, \dots, s_{n-1})$ ja osoitetaan, että se pätee myös $(n+1)$-pituisilla jonoilla $(s_0, \dots, s_n)$. Tällöin

$$\begin{aligned} g\alpha^{s_0} \cdots g\alpha^{s_n} &= (\alpha_1^{s_0}\alpha_2^{s_1} \cdots \alpha_n^{s_{n-1}} g^n) g\alpha^{s_n} \\ &= \alpha_1^{s_0}\alpha_2^{s_1} \cdots \alpha_n^{s_{n-1}} g^{n+1}\alpha^{s_n}(g^{n+1})^{-1}g^{n+1} \\ &= \alpha_1^{s_0}\alpha_2^{s_1} \cdots \alpha_{n+1}^{s_n} g^{n+1}. \end{aligned}$$

Tästä saadaan yhtäsuuruus

$$g\alpha^{s_0} \cdots g\alpha^{s_m} = \alpha_1^{s_0}\alpha_2^{s_1} \cdots \alpha_{m+1}^{s_m} g^{m+1}. \tag{6.3.2}$$

Yhtälön (6.3.2) avulla ominaisuus (6.3.1) voidaan ilmaista muodossa

$$\alpha_1^{s_0} \cdots \alpha_{m+1}^{s_m} g^{m+1} = \alpha_1^{t_0} \cdots \alpha_{m+1}^{t_m} g^{m+1},$$

mistä voidaan vielä päätellä

$$\alpha_1^{s_0} \cdots \alpha_{m+1}^{s_m} = \alpha_1^{t_0} \cdots \alpha_{m+1}^{t_m}.$$

Lähdetään tämän avulla osoittamaan, että jokainen α_n, $n > m$, voidaan ilmaista pelkästään alkioilla $\alpha_1, \dots, \alpha_m$. Koska $s_m \neq t_m$, niin $s_m - t_m = \pm 1$, jolloin aiemman nojalla

$$\alpha_1^{s_0} \cdots \alpha_{m+1}^{s_m - t_m} = \alpha_1^{t_0} \cdots \alpha_m^{t_{m-1}},$$

mikä voidaan vielä muokata muotoon

$$\alpha_{m+1}^{\pm 1} = \alpha_m^{-s_{m-1}} \cdots \alpha_2^{s_1}\alpha_1^{t_0 - s_0} \cdots \alpha_m^{t_{m-1}}. \tag{6.3.3}$$

Konjugoimalla tätä yhtälöä molemmilta puolilta alkiolla g saadaan

$$\begin{aligned} \alpha_{m+2}^{\pm 1} &= g(\alpha_m^{-s_{m-1}} \cdots \alpha_2^{s_1}\alpha_1^{t_0 - s_0} \cdots \alpha_m^{t_{m-1}})g^{-1} \\ &= \alpha_{m+1}^{-s_{m-1}} \cdots \alpha_3^{s_1}\alpha_2^{t_0 - s_0} \cdots \alpha_{m+1}^{t_{m-1}}. \end{aligned}$$

Yhtälön (6.3.3) nojalla α_{m+1} voidaan ilmaista alkioiden $\alpha_1, \dots, \alpha_m$ potenssien tulona. Näin ollen myös α_{m+2} voidaan ilmaista näiden avulla.

Jatkamalla näin induktiivisesti voidaan päätellä, että jokaisella $k \geq m+1$ alkio α_k, voidaan ilmaista alkioilla $\alpha_1, \dots, \alpha_m$. Näin ollen jokainen α_n, $n \in \mathbb{N}$, voidaan ilmaista alkioilla $\alpha_1, \dots, \alpha_m$. Konjugoimalla yllä olevassa päättelyssä alkiolla g^{-1} alkion g sijasta saadaan pääteltyä, että alkio α_n voidaan ilmaista alkioiden $\alpha_1, \dots, \alpha_m$ avulla jokaisella $n \in \mathbb{Z}$.

Näin ollen jokainen aliryhmän N virittäjä α_n kuuluu joukon $\{\alpha_1, \ldots, \alpha_m\}$ virittämään ryhmään N'. Koska N on pienin ryhmä, joka sisältää joukon $\{\alpha_k \mid k \in \mathbb{Z}\}$ täytyy päteä, että $N = N'$. Näin ollen N on äärellisesti viritetty. $\square$

Lause 6.4. Olkoon
$$1 \to A \to G \xrightarrow{\pi} H \to 1$$
lyhyt eksakti jono, A vaihdannainen ryhmä ja G äärellisesti viritetty ryhmä. Jos H on polysyklinen, niin G on joko polysyklinen tai se kasvaa eksponentiaalisesti.

Todistus. Oletetaan, että G kasvaa subeksponentiaalisesti ja osoitetaan, että tällöin G on polysyklinen. Lähdetään osoittamaan, että A on äärellisesti viritetty. Tällöin A on äärellisesti viritettynä ja vaihdannaisena ryhmänä polysyklinen. Koska A on polysyklinen ja $G/A \cong H$ on polysyklinen, niin lauseen 5.27 nojalla ryhmä G on tällöin polysyklinen.

Koska H on polysyklinen, niin lauseen 5.24 nojalla H on äärellisesti viritetty. On siis olemassa sellaiset $h_1, \ldots, h_q \in H$, että jokainen $h \in H$ on muotoa $h = h_1^{m_1} \cdots h_q^{m_q}$, missä $m_1, \ldots, m_q \in \mathbb{Z}$. Kuvaus π on surjektio, joten jokaisella $i \in \{1, \ldots, q\}$ voidaan valita sellaiset $g_i \in G$, että $\pi(g_i) = h_i$. Jonon eksaktiudesta johtuen ryhmien A ja G välillä on injektio, joten A voidaan ajatella ryhmän G normaalina aliryhmänä. Jonon eksaktiudesta seuraa, että $A = \ker \pi$, joten homomorfialauseen nojalla $G/A \cong H$.

Jos alkiot $g \in G$ ja $h \in H$ ovat sellaisia, että $\pi(g) = h$, niin $\pi(g) = \pi(g_1^{m_1} \cdots g_q^{m_q})$, joten sivuluokille pätee $gA = g_1^{m_1} \cdots g_q^{m_q} A$. Tällöin $g \in g_1^{m_1} \cdots g_q^{m_q} A$, eli $g = g_1^{m_1} \cdots g_q^{m_q} a$ jollain $a \in A$.

Lauseen 6.1 nojalla ryhmällä H on näin ollen äärellinen esitys. Tällöin lauseen 6.2 nojalla on olemassa sellainen äärellinen osajoukko $A' = \{a_1, \ldots, a_k\} \subset A$, että $A = \langle\langle A' \rangle\rangle$. Näin ollen lauseen 3.7 nojalla jokainen $a \in A$ on äärellinen tulo alkioiden a_j konjugaatteja $g a_j g^{-1}$, missä $g \in G$. Tällöin ryhmän A vaihdannaisuudesta ja $g = g_1^{m_1} \cdots g_q^{m_q} a$ seuraa, että
$$\begin{aligned} g a_j g^{-1} &= (g_1^{m_1} \cdots g_q^{m_q} a) a_j (g_1^{m_1} \cdots g_q^{m_q} a)^{-1} = g_1^{m_1} \cdots g_q^{m_q} (a a_j a^{-1}) g_g^{-m_q} \cdots g_1^{-m_1} \\ &= g_1^{m_1} \cdots g_q^{m_q} a_j (g_1^{m_1} \cdots g_q^{m_q})^{-1}. \end{aligned}$$

Lauseen 6.3 nojalla joukon $\{g_q^m a_i g_q^{-m} \mid a_i \in A', m \in \mathbb{Z}\}$ virittämä ryhmä A_q on äärellisesti viritetty. Olkoon S_q ryhmän A_q äärellinen virittäjäjoukko. Olkoon A_{q-1} joukon $\{g_{q-1}^n s g_{q-1}^{-n} \mid s \in S_q, n \in \mathbb{Z}\}$ virittämä ryhmä. Nyt jokainen muotoa

$g_{q-1}^n g_q^m a_i g_q^{-m} g_{q-1}^{-n}$ oleva alkio kuuluu ryhmään A_{q-1}. Jälleen lauseen 6.3 nojalla A_{q-1} on äärellisesti viritetty. Olkoon S_{q-1} ryhmän A_{q-1} äärellinen virittäjäjoukko.

Jatkamalla induktiivisesti voidaan päätellä, että joukon $\{g_1^m s g_1^{-m} \mid s \in S_2\}$ virittämä ryhmä A_1 on lauseen 6.3 nojalla äärellisesti viritetty. Olkoon S_1 ryhmän A_1 äärellinen virittäjäjoukko. Jokainen muotoa $g_1^{m_1} \cdots g_q^{m_q} a_j (g_1^{m_1} \cdots g_q^{m_q})^{-1}$ oleva alkio kuuluu ryhmään A_1, joten $A \subset A_1$. Tästä seuraa, että $A = A_1$, joten ryhmä A on äärellisesti viritetty.

Näin ollen jos ryhmä G kasvaa subeksponentiaalisesti, ryhmä A on äärellisesti viritetty. Tällöin A on äärellisesti viritettynä vaihdannaisena ryhmänä polysyklinen. Lauseen 5.27 nojalla ryhmä G on polysyklinen. □

Lause 6.5 (Milnor)**.** Äärellisviritteinen ratkeava ryhmä on joko polysyklinen tai kasvaa eksponentiaalisesti.

Todistus. Olkoon G äärellisviritteinen ratkeava ryhmä. Todistetaan väite induktiolla pienimmän luvun d suhteen, jolle pätee $G^{(d)} = \{1_G\}$. Oletetaan aluksi, että $d = 1$. Tällöin $G^{(1)} = G' = \{1_G\}$, eli G on vaihdannainen ja äärellisesti viritetty. Esimerkin 5.22 perusteella G on polysyklinen.

Olkoon nyt $d \in \mathbb{N}$ sellainen luku, että jos G on äärellisesti viritetty ratkeava ryhmä, jolla pienin sellainen k, että $G^{(k)} = \{1_G\}$, $k \leq d$, niin tällöin joko G kasvaa ekspontiaalisesti tai on polysyklinen. Osoitetaan väite myös luvulle $d+1$. Olkoon G sellainen äärellisesti viritetty ja ratkeava ryhmä, että $d+1$ on pienin luku, jolla $G^{(d+1)} = \{1_G\}$. Aliryhmät $G^{(k)}$ ovat karakteristisia ryhmässä G, joten voidaan muodostaa tekijäryhmä $H := G/G^{(d)}$, joka on myös äärellisesti viritetty. Olkoon $\pi : G \to G/G^{(d)}$ tekijäkuvaus. Lauseen 5.10 nojalla $\pi(G^{(i)}) = (G/G^{(d)})^{(i)}$. Erityisesti H on ratkeava, sillä

$$\left(G/G^{(d)}\right)^{(d)} = \pi\left(G^{(d)}\right) = G^{(d)} = 1_{G/G^{(d)}}.$$

Lisäksi pienimmälle luvulle k, jolla $H^{(k)}$ on triviaali pätee $k \leq d$, joten induktio-oletuksen nojalla H on joko polysyklinen tai se kasvaa eksponentiaalisesti. Jos H kasvaa eksponentiaalisesti, niin lauseen 4.20 nojalla myös G kasvaa eksponentiaalisesti.

Jos H on polysyklinen, niin lauseen 6.4 todistusta mukaillen voidaan päätellä, että G on joko polysyklinen tai se kasvaa eksponentiaalisesti. Ryhmistä G, $G^{(d)}$ ja H voidaan muodostaa lyhyt eksakti jono, joka on muotoa

$$1 \to G^{(d)} \hookrightarrow G \xrightarrow{\pi} H \to 1,$$

missä $G^{(d)} \hookrightarrow G$ on inkluusiokuvaus. Oletusten nojalla G on äärellisesti viritetty ja $G^{(d+1)} = \left(G^{(d)}\right)' = \{1_G\}$, eli aliryhmä $G^{(d)}$ on vaihdannainen. Ryhmä H on polysyklinen, joten sillä on lauseen 6.1 nojalla jokin äärellinen esitys. Tällöin lauseen 6.2 nojalla on olemassa sellainen äärellinen osajoukko $A \subset G^{(d)}$, että $G^{(d)} = \langle\langle A \rangle\rangle$. Jos ryhmä G kasvaa subeksponentiaalisesti, niin voidaan päätellä, että aliryhmä $G^{(d)}$ on äärellisesti viritetty. Tällöin aliryhmä $G^{(d)}$ on äärellisesti viritettynä ja vaihdannaisena ryhmänä polysyklinen. Lisäksi $H = G/G^{(d)}$ oletettiin polysykliseksi, joten lauseen 5.27 nojalla ryhmä G on polysyklinen. Muussa tapauksessa ryhmä G kasvaa eksponentiaalisesti.

Näin ollen jos $G^{(d+1)} = \{1_G\}$, niin ryhmä G joko kasvaa eksponentiaalisesti tai on polysyklinen. □

Wolfin lauseen [2, theorem 14.30] nojalla jokainen polysyklinen ryhmä on joko *melkein* nilpotentti tai se kasvaa eksponentiaalisesti. *Melkein* nilpotentit ryhmät ovat ryhmiä, joilla on jokin äärellisen indeksin aliryhmä, joka on nilpotentti (ks. määritelmä 2.17). Milnorin ja Wolfin tulokset voidaan yhdistää yhteiseksi tulokseksi, joka kertoo, että äärellisesti viritetyt ratkeavat ryhmät kasvavat joko polynomisesti tai eksponentiaalisesti.

Lause 6.6 (Milnor-Wolf)**.** Jokainen äärellisesti viritetty ratkeava ryhmä on joko *melkein* nilpotentti tai kasvaa eksponentiaalisesti.

Nilpotenttien ryhmien on osoitettu kasvavan polynomisesti [2, Bass-Guivarc'h Theorem]. Lisäksi ryhmät ja niiden äärellisen indeksin aliryhmät kasvavat samaan tahtiin [2, proposition 8.78(b)], joten myös jokainen *melkein* nilpotentti ryhmä kasvaa polynomisesti. Näin ollen Wolfin lauseen nojalla jokainen polysyklinen ryhmä kasvaa joko polynomisesti tai eksponentiaalisesti. Milnorin lauseen nojalla jokainen äärellisesti viritetty ratkeava ryhmä joko kasvaa eksponentiaalisesti tai on polysyklinen. Näin ollen jokainen äärellisesti viritetty ratkeava ryhmä kasvaa joko polynomisesti tai eksponentiaalisesti.

Kirjallisuutta

[1] James W. Cannon. *Handbook of geometric topology, Chapter 6: Geometric group theory.* Elsevier Science B.V. 2002.

[2] Cornelia Druțu, Michael Kapovich: *Geometric group theory.* American Mathematical Society, Colloquium Publications Volume 63, 2018.

[3] Rostislav I. Grigorchuk: *On the Milnor problem of group growth.* Dokl. Akad. Nauk SSSR 271, no. 1, 30–33, 1983.

[4] Mikhael Gromov: *Groups of polynomial growth and expanding maps.* Publications mathématiques de l'I.H.É.S 53, 53-73, 1981.

[5] Einer Hille, Ralph S. Phillips: *Functional analysis and semi-groups.* American mathematical society, Colloquium Publications Volume 31, 1957.

[6] Jokke Häsä: *Algebra II* luentomuistiinpanot kevät 2010 (korjattu 2016), Helsinki, Helsingin yliopisto

[7] Jokke Häsä, Johanna Rämö: *Johdatus abstraktiin algebraan*, 3. painos. Gaudeamus Helsinki University Press, 2012.

[8] John Milnor: *Growth of finitely generated solvable groups.* Journal of Differential Geometry. 2(4), 447-449, 1968.

[9] Joseph J. Rotman: *An introduction to the theory of groups, Fourth Edition.* Graduate texts in mathematics, Springer, New York, NY, 1999.

[10] William R. Scott: *Group theory.* Prentice-Hall, Inc. Englewood Cliffs, N.J., 1964.

[11] Jean-Pierre Serre: *Trees.* Springer Monographs in Mathematics, Springer, New York, NY, 1980.

[12] Joseph A. Wolf : *Growth of finitely generated solvable groups and curvature of Riemannian manifolds.* Journal of Differential Geometry. 2(4), 421-446, 1968.